Service user guide

BACSTEL-IP

BACS

About this guide

This guide is for people that use BACSTEL-IP® to access the BACS® electronic funds transfer (EFT) service. It provides an overview of the EFT service and information on how to use this service.

This guide includes your *Contact's guide* for BACS payment services. This takes you through the basics of the BACS payment services website, one of your interfaces with BACSTEL-IP. The *Contact's guide* starts on page 69.

Other guides

Use this guide along with any documentation from your sponsor and, if applicable, your solution supplier.

There are also two getting started guides for you, depending on whether you are a direct submitter or an indirect submitter. These cover every day tasks on payment services to help you get started quickly. You can get these guides from *www.bacstel-ip.com* (select General information, then Post migration).

Service desk information

t 0870 010 0698

t 0870 165 0018

e *servicedesk@BacsServices.co.uk*

Telephone calls to the BACS service desk may be recorded for security or monitoring purposes.

Our reference PN3763
Released 2 June 2005
Version 2.00

This document is issued by Voca Limited on behalf of BACS Payment Schemes Limited for use by users in connection with BACSTEL-IP but not otherwise. This document shall not be used, distributed or otherwise disclosed or copied (whether in whole or part) for any other purpose without the express written permission of BACS Payment Schemes Limited.

All material, concepts and ideas detailed in this document are confidential to BACS Payment Schemes Limited.

This document is issued "as is" and without any warranty that it is accurate or error free or regarding its suitability or fitness for purpose. In the event that the document contains any material error or inaccuracy or is misleading in any material respect, on being so notified BACS Payment Schemes Limited shall use reasonable endeavours to amend the document to remedy the position. This represents BACS Payment Schemes Limited's only obligation and, in the case of any person who uses or relies on this document, that person's exclusive remedy, in the event that the document is erroneous, inaccurate or misleading. Subject to that obligation, neither Voca Limited or BACS Payment Schemes Limited accepts any liability whatsoever (whether contractual, tortious or otherwise) to any person arising out of or relating to that person's use of, or reliance upon, the information contained in this document or any service, or unavailability of any service, described in this document.

Contents

Part I

About the EFT service

Part II

Your structure

Part III

Your BACSTEL-IP software

Part IV

Service user information

Part XII

Your details

Glossary

Part I

About the EFT service

The electronic funds transfer (EFT) service allows registered users to make or collect payments and set up and cancel Direct Debit Instructions (DDIs) on people's accounts. To use this service you are sponsored by a bank or building society that is a scheme member of BACS clearing.

This part gives you an overview of the EFT service and the BACSTEL-IP service.

Your sponsoring bank or building society sets up information about your company so you can access payment services. For information on this set up, see part II, starting on page 19.

Two of the key services offered are:

- Direct Debit – allowing you to collect agreed regular and ad hoc payments
- Direct Credit – allowing you to pay money into people's accounts. This could be wages or ad hoc payments such as invoices.

For more information on these services and the services to support these, please speak to your sponsor or go to *www.bacs.co.uk*

1 Sending payment information

To make or collect payments or set up/cancel Direct Debit Instructions (DDIs), you use “payment instructions”. These payment instructions contain information about the type of transaction, the value and where the money is coming from and where it is going to.

Payment instructions are sent in “payment files” that are sent to the BACS service in “submissions”.

This information must be in APACS Standard 18 format. This standard specifies the contents and lengths of each field and record in a submission, payment file and payment instruction. If you use BACS approved software for BACSTEL-IP to create submissions, your software is designed to use the Standard 18 format.

1.1 Payment instructions

Payment instructions contain details of the transaction you want to make; paying money into someone’s account (credits) or collecting money (debits).

If you are an AUDDIS® (Automated Direct Debit Instruction Service) originator, you also use payment instructions to inform a bank or building society to set up or cancel a DDI on someone’s account. For information on AUDDIS, contact your sponsor.

The table below describes the key contents of payment instructions.

Content	Detail
Originating account details	This is your account. If this is a credit transaction, this is the account that the money is paid from; if this is a debit, this is where the money is paid into.
Destination account details	This is the account that the transaction is directed to. For a credit, this is where the money is paid into; for a debit, this is where the money is collected from; for a DDI, this is the account that the instruction is applied on.
Transaction code	A two character code that represents the type of transaction you are making. For a list of transactions, see the following page.
Value of payment	The amount in pence (for sterling) or cents (for euro) of the transaction. (The currency is set as part of the payment file.) *Note: DDIs have no value; therefore this is set to zero for DDIs.*
Reference information	Additional reference information is held in several fields; for example, a Direct Debit reference.

The date a payment instruction is to be processed can be set for the whole payment file or for each payment instruction.

Transaction types

Below are the transaction types that are recognised by the BACS service (other transactions are also recognised for bank grade users, speak to your sponsor for information on these if you are bank grade). You can normally only originate some of these transaction types. If you are not sure the transactions you are set up to use, speak to your sponsor. The transaction codes listed are used in the payment instruction to identify the transaction.

Transaction code	Transaction type	Credit or debit
99	Direct Credit	Credit
99	Debit contra (a credit record to balance debit records)	Credit
17	Credit contra (a debit record to balance credit records)	Debit
01	Direct Debit – first collection	Debit
17	Direct Debit – regular collection	Debit
18	Direct Debit – re-presentation	Debit
19	Direct Debit – final collection	Debit
0N	Direct Debit Instruction – new instruction	No value
0C	Direct Debit Instruction – cancellation instruction	No value
0S	Direct Debit Instruction – conversion instruction	No value
Z4	Interest payments	Credit
Z5	Dividend payments	Credit
E1	Credit card debit	Debit
E2	Credit card refund	Credit

1.2 Payment files

Payment files contain payment instructions. A payment file submitted over BACSTEL-IP can contain a mix of credits, debits and DDIs. All payment files have a processing date. This date can be up to 31 days later than the current processing date. Payment files can be either:

- **Single processing day files –** All payment instructions in the payment file are processed on the file's processing date. The payment instructions themselves do not have processing dates set against them
- **Multiprocessing day files –** Each payment instruction has its own processing date. This can be the same as, or up to 39 days after, the processing date in the payment file.

The payment file also sets the currency of the payment instructions; sterling or euro. This means all payment instructions in a file will be the same currency. The BACS service currently allows sterling credit and debit transactions and euro credit transactions. (BACS does not carry out any conversion on euro transactions. However, some banks/building societies may convert a euro transaction to sterling when they apply it to a person's account.)

Day sections

The payment instructions in a payment file with the same processing date are known as a "day section". A single processing day file is made up of one day section because all the payment instructions are processed on the same day. You get an input report to confirm processing of day sections; so for a multiprocessing day file, you may get multiple input reports.

Account sections and balancing

In each day section, the payment instructions that are originated from the same account form an "account section". Details of these account sections appear on your input report.

Each account section in a payment file must balance. This is done using contras. A contra is a type of payment instruction; the destination and originating accounts are the same (this is to identify the account section that the contra is balancing). The word "contra" is included as part of the payment instruction to identify it.

Debits and credits in an account section need separate contras. Credit contras balance credit payment instructions; the credit contra takes money from your account. Debit contras balance debit payment instructions; the debit contra deposits money into your account.

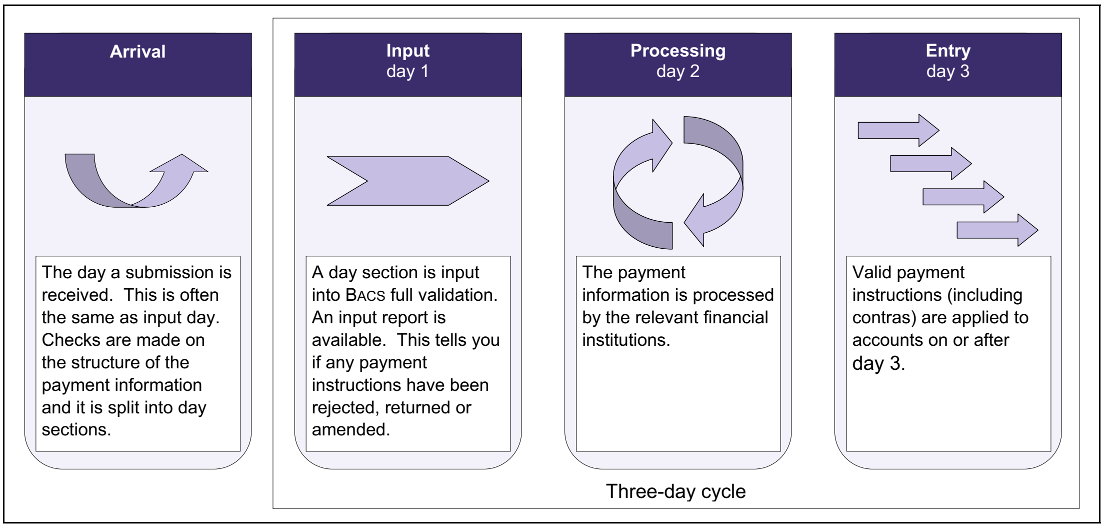
1.3 Submissions

Payment files are sent in "submissions". A bureau can send more than one file in a submission. A service user can only send one payment file in a submission.

2 Processing cycle and opening times

The processing cycle is the minimum time it takes between a payment instruction being input by BACS for validation and the payment instruction being applied to the destination account.

The processing cycle has three stages that take place on three consecutive processing days; this is the three-day cycle. In addition, “arrival” is the stage that a submission is received by the BACS service and divided into day sections. This is often the same day as the input stage.



The day a submission is received. This is often the same as input day. Checks are made on the structure of the payment information and it is split into day sections.

A day section is input into BACS full validation. An input report is available. This tells you if any payment instructions have been rejected, returned or amended.

The payment information is processed by the relevant financial institutions.

Valid payment instructions (including contras) are applied to accounts on or after day 3.

Figure 1: The three-day cycle

2.1 Processing and nonprocessing days

Input, processing and entry can only occur on processing days. Nonprocessing days are Saturdays, Sundays and English bank/public holidays. These dates are highlighted on the processing calendar. This is available on the internet at *www.bacs.co.uk/resources*

The processing calendar also highlights bank holidays in Northern Ireland that can affect entry day for accounts held in Northern Ireland. The calendar shows the Julian date for each processing day. This is the date format used in submissions.

Use the calendar to ensure you only use valid processing dates in your payment files and payment instructions. If you use invalid processing dates, BACS overrides the processing date according to certain rules. When you send a submission using BACSTEL-IP with an invalid processing date, you receive a warning message saying that date(s) have been overridden. Read these messages carefully and if you have any concerns contact your sponsor.

2.2 Processing stages

The table below describes the stages your payment information goes through and what can happen to your payments. For more information on the reports and how to access them, see part V, starting on page 43.

Stage	What can happen	How you are notified
Arrival		
When you send a submission, while your software is still connected to BACSTEL-IP, initial checks are made on the content of your submission.	Submissions can be: • *Accepted* – if any processing days are invalid they may be amended during processing, your submission summary report tells you how dates will be changed • *Rejected* – no information is processed.	A *submission summary report* is sent to your BACSTEL-IP software. You can also view this information by checking your submissions on payment services, see sec 13, pg 55.
After the submission has been accepted by BACSTEL-IP, more checks are made on it. (When a day section reaches its processing cycle, it goes to the next stage.)	Submissions can be: • *Accepted* • *Rejected* – no information is processed.	If the submission is rejected at this stage, the submitter receives an *arrival report*.
Input		
Payment instructions are validated before accepted and amended instructions are passed to the relevant banks/ building societies. This occurs on day 1 of the 3-day cycle.	Payment instructions can be: • *Accepted* • *Amended* – if you use an incorrect date on a payment instruction, it will be amended. The payment will still be processed • *Returned* – the payment is returned to you • *Rejected* – the payment is not processed and an “adjustment item” is created so your day section still balances.	The originator receives an *input report* for each day section. Input reports list returned, rejected and amended payment instructions.
Processing and entry		
The recipient banks/building societies carry out further processing on day 2 before applying valid instructions on day 3 (or after).	Payment instructions can be: • *Applied* • *Unapplied* – the payment is returned to you, normally using ARUCS (automated return of unapplied credits service) or ARUDD (automated return of unpaid Direct Debits). If a DDI cannot be applied, you are notified on an AUDDIS report.	If payments are returned using ARUCS or ARUDD, the originator receives an *ARUCS* or *ARUDD report*. If the account details of a payment had to be amended by the bank/building society before they could apply the payment, you may be notified using an *AWACS (advice of wrong account for automated credits service)* or *ADDACS® (Automated Direct Debit Amendment and Cancellation Service) report*.

2.3 Service opening times

BACSTEL-IP and payment services are currently open from 07:00 hours on Monday through to 23:00 hours on Friday, although it is impacted by English bank/public holidays; you can make submissions over BACSTEL-IP from 07:00 hours Monday to 22:30 hours Friday. (These times are configurable and so could change.)

If you try to access the service when it is closed, you receive a message saying the service is closed.

Each day that the service is open there is a current processing day deadline. This is currently 22:30 hours. This is the time that all submissions for the current processing day must be received by the BACS service. Looking at the processing cycle in figure 1, this means if you have payment information to be processed on day 2 (for entry into people's accounts on day 3), it must be received by 22:30 hours on day 1.

All submissions in progress at 22:30 hours that are for the current processing day will be assessed. While efforts will be made to accommodate the transmission, the submission may have to be terminated or passed for processing on the next available day. Before any action is taken, we will attempt to get in touch with a contact at the service user. If a submission is terminated, or if the processing day is changed, information will also be included in the submission summary that is sent to your BACSTEL-IP software, see section 7.4, page 28. You can also view this information on payment services, see section 13, page 55.

Service closure – English bank/public holidays

The service is closed on English bank/public holidays.

The following is an example of how this affects the opening of BACSTEL-IP:

- If Monday is a bank holiday, the service is closed on Monday and opens at 07:00 hours on Tuesday
- If Friday is a bank holiday, the service is closed from 23:00 hours on Thursday
- If Wednesday is a bank holiday, the service is closed from 23:00 hours on Tuesday and opens at 07:00 hours on Thursday (it then closes as normal at 23:00 hours on Friday).

3 Using BACSTEL-IP

BACSTEL-IP is your access channel to the BACS electronic funds transfer service. There are two ways you can access BACSTEL-IP:

- **Using the BACS payment services website** – using a web browser, you can log on to payment services to:
  - Access your processing reports
  - View information about your submissions
  - View and maintain certain information about your service user, including adding contacts (see part II, starting on page 19 for more information about service users and contacts)
- **Using your BACS approved software for BACSTEL-IP** – you can:
  - Send submissions
  - Access your processing reports.

Only people that send payment information directly to BACS normally use software to connect to BACSTEL-IP.

For general information on the payment services website, see the *Contact's guide*, starting on page 69. For information on using software with BACSTEL-IP, see part III, starting on page 25.

Security

To use BACSTEL-IP, you need security credentials. There are two types that can be used:

- Public key infrastructure (PKI) credentials
- Contact ID and password security, called ASM (alternative security method).

There are two ways you can use PKI security with BACSTEL-IP:

- With a **smartcard** – you use a smartcard by inserting it into a smartcard reader and using a PIN to digitally sign information that is displayed to you
- With a **hardware security module (HSM)** – an HSM is a piece of hardware that is installed into your computer systems and is used to hold PKI credentials. HSMs allow you to automate your submission and report access process. Using an HSM means you do not need someone present to enter their smartcard and PIN. HSMs are only used with your BACSTEL-IP software. They are mainly used by organisations that make frequent submissions or need to automate the process. You will still use smartcards if you need PKI access to the payment services website.

PKI is the only security that can be used with your BACSTEL-IP software. The *Contact's guide,* starting on page 69, has more information about these security methods.

Connecting to BACSTEL-IP

You can connect to BACSTEL-IP (using your software or payment services) using:

- The internet, using any internet service provider (ISP)
- The dial-up extranet, using a modem and a phone line or ISDN line. You dial into an 0870 number. To do this you need an extranet ID and password. See the *Contact's guide,* section 24.2, page 80 for more information
- A number of products offering always on, high speed connections:
  - Fixed Extranet Connect
  - DSL Connect
  - Broadband Direct.

For comparisons of these connection methods, including the submission speeds you can expect, go to www.bacstel-ip.com (go to *Direct submitters*, and select *Downloads*). This also contains information about how to order Fixed Extranet Connect, DSL Connect and Broadband Direct.

You do not always have to connect using the same connection method. You may also want to use different methods for connecting to payment services and the BACSTEL-IP software channel; for example, you may want to connect to payment services using the internet and BACSTEL-IP using Broadband Direct.

Contingency planning

You must consider your contingency needs. You should make sure you have no single points of failure that could stop you from sending payment information.

When assessing your needs, consider the impact if you could not submit a file. The business implications and the associated costs of such a problem need to be considered when deciding on contingency solutions.

We recommend that all users have a relationship set up with a bureau that can submit on your behalf if needed. Your bank or software supplier may offer bureau services or you can go to another organisation that offers a bureau service. Any organisation that provides bureau services to third parties must be a BACS Approved Bureau, so you know they meet set standards.

You must inform your bank of the details of any bureau you may use to submit, before a file is submitted by them. If a bureau that is not linked to you submits a file on your behalf then the file will be rejected (unless you have digitally signed the file, see section 7.2, page 27 for information on signing payment files).

Some bureau may also offer a service to collect your reports from payment services on your behalf. Your sponsor needs to set up permissions to allow a bureau to do this for you.

You should also consider the following:

- Connection problems – you should have other ways to connect, for example a spare telephone line to connect using a dial-up connection
- A contact's smartcard does not work or a contact is off sick or on holiday – you should always have multiple contacts with smartcards and the necessary privileges
- The computer with your BACSTEL-IP software fails – under your licensing arrangements, you may be able to have backup installations of your software; speak to your supplier.

If you have multiple sites, you may consider having people at different sites that are set up as contacts for your service user. If you use an HSM, you may also consider having the ability to submit using a smartcard as a backup (not all software will support this) or having a second HSM. You should speak to your supplier or your bank for advice when considering contingency for HSMs.

Part II

Your structure

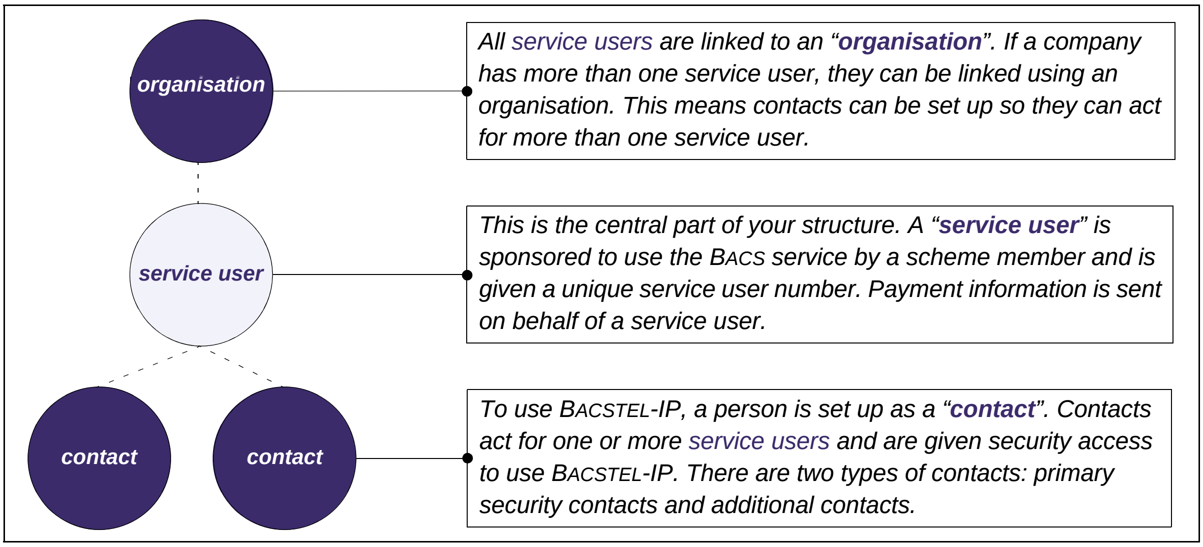
This part describes how you are set up on BACSTEL-IP to use payment services. It tells you about your structure and the information held about your service user.

A company is sponsored to use payment services by a bank/building society that is a scheme member of BACS clearing[1]. You can transfer your sponsorship to another scheme member.

[1] *In this part, company is used to refer to a company, a part of a company (such as the payroll section), a group of companies, a charity or any other body that can be set up to access BACS payment services.*

4 Overview of your structure

When a company is set up to use payment services, your sponsor sets up three basic parts.



*All service users are linked to an "**organisation**". If a company has more than one service user, they can be linked using an organisation. This means contacts can be set up so they can act for more than one service user.*

*This is the central part of your structure. A "**service user**" is sponsored to use the BACS service by a scheme member and is given a unique service user number. Payment information is sent on behalf of a service user.*

*To use BACSTEL-IP, a person is set up as a "**contact**". Contacts act for one or more service users and are given security access to use BACSTEL-IP. There are two types of contacts: primary security contacts and additional contacts.*

Figure 2: A service user's structure

4.1 Organisation

An organisation is the top level of your structure. It groups service users that are part of the same company, group of companies etc. (Most organisations will only have one service user.)

The advantage of grouping service users together in an organisation is that it allows contacts to be linked to more than one service user – to do this, service users have to have the same sponsor. For example, your payroll and finance sections may be set up as two different service users. If they are in the one organisation, then a contact could be linked to both service users. This means the contact could submit, collect reports etc for both service users, using the same smartcard. Speak to your sponsor if you have service users that you think should be grouped together.

4.2 Service user

A service user is the central part of your structure. It is identified by a unique service user number. For regular service users, this is six numerals. For bureau service users, this is the letter B followed by five numerals.

As a service user you are given a "licence" to use the BACS three-day service. This licence holds information about the accounts you use to originate payments and software packages (if any) that you can use to send submissions. For more information about service users and the BACS three-day licence, see section 5, page 22.

4.3 Contacts

Contacts are the people that act for the service user. They are given “privileges” to allow them to do certain things for that service user. For example, contacts can be given a privilege to access processing reports and/or make submissions.

Contacts are also given security credentials – PKI credentials and/or ASM.

Contacts are always linked to at least one service user. If there are multiple service users with the same sponsor and in the same organisation, then a contact can be linked to more than one service user. If you are linked to more than one service user, you use the same security for all service users and you have the same privileges.

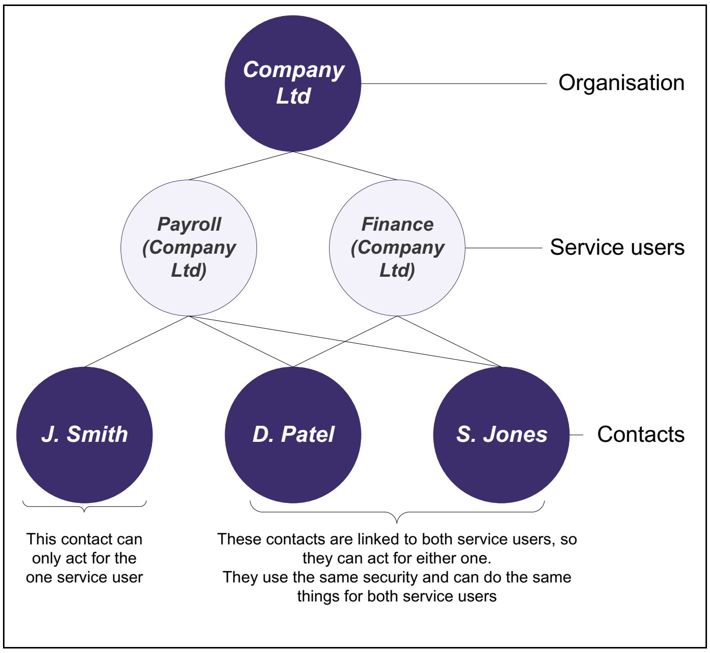

Company Ltd
Organisation
Payroll (Company Ltd)
Finance (Company Ltd)
Service users
J. Smith
D. Patel
S. Jones
Contacts
This contact can only act for the one service user
These contacts are linked to both service users, so they can act for either one.
They use the same security and can do the same things for both service users

Figure 3: An organisation with two service users sharing contacts

There are two types of contact:

- **Primary security contacts**
  Direct submitters must have at least two primary security contacts (PSCs). PSCs can be given privileges so they can add and maintain additional contacts in their service user and also maintain certain information held about their service user. (There are no privileges that can be given to additional contacts that cannot be given to PSCs.) PSCs can only be added and maintained by your sponsor. PSCs receive notification emails when certain things happen on BACSTEL-IP. These emails relate to changes made to your service user and any additional contacts and if submissions are rejected.

- **Additional contacts**
  There is no minimum requirement for additional contacts. Additional contacts can be given privileges related to making submissions and reports.

For information on how PSCs add and maintain additional contacts and also details of available privileges, see part VI, starting on page 57.

5 Service users and the three-day licence

Service users are given a “licence” to use the BACS three-day service. This licence holds various information about your service user.

5.1 Service user type

Your service user is one of two types:

Type	Information
Service users	Service users can originate payment instructions: a direct submitter service user, see section 5.2, page 22, can also send submissions. Service users have information such as originating account information held about them.
Bureaux	Bureaux can submit payment instructions on behalf of service users. They cannot originate payment instructions themselves. Some bureaux create the payment file for the service user, others just submit payment files given to them by a service user. To submit payment files for a service user: • There must be a relationship set up by the sponsor of the service user with the bureau; **or** • The payment file must be digitally signed by a contact at the service user, see “Payment file signatures” on page 27. Bureaux that submit on behalf of third parties must be approved by BACS. These are called commercial bureaux. A bureau can be set up to access reports on behalf of a service user; for more information see section 10.3, page 45.

5.2 Service user role

Your service user has one of two roles.

Role	Information
Direct submitter	Direct submitters send payment files directly to BACS. A direct submitter that is a service user (rather than a bureau) can also originate payment information. All bureaux are direct submitters.
Indirect submitter	Indirect submitters can instruct a bureau to submit a payment file to BACS on their behalf. This file uses the indirect submitter’s service user number and originates payment instructions from originating accounts belonging to the indirect submitter.

Note: It is recommended that direct submitter service users have a relationship set up with one or more bureaux for contingency. If the service user cannot connect to BACS themselves for some reason, the bureau can submit payment information on their behalf. If you are a direct submitter and have no relationship with a bureau, please speak to your sponsor.

6 Account structure

The accounts you use to originate payment instructions must be set up as part of your account structure. Bureaux cannot originate payment instructions so do not have an account structure.

In some cases, you may be able to have some accounts held at a bank/building society other than your sponsor; speak to your sponsor for information. If you do have accounts held at other banks, you still only have PKI credentials issued by your sponsor – these are used when making submissions regardless of the accounts being originated from.

You can see your accounts on payment services; see section 9.2, page 39.

6.1 Account types

Accounts are categorised into the following types:

- Main
- Individual
- Group main
- Group individual.

The maximum number of accounts you can have is 30. The minimum you can have is one main account and one individual account. These two accounts could have the same account details (that is, they are the same sorting code and account number) but are set up by your sponsor as two accounts in your structure.

6.2 Function of the accounts

The table below describes the function of each account type.

Type	Function
Main	This is the top account in your hierarchy. If you try to originate a payment instruction from an account you are not set up to use, BACS substitutes the details of the main account.
Individual	You use this to originate payment instructions (including contras).
Grouped – group main and group individual	The group main account groups together two or more group individual accounts. You originate payment instructions from group individual accounts. When it comes to balancing the account section, the group main account must balance. For example, you could originate £100 in credits from one group individual account and direct a £100 credit contra to another group individual account in the same group. *Note: Most service users will not have any reason to use group accounts.*

Normally, when a payment instruction is returned to you by BACS because it fails validation (during the input stage described in the table on page 14), it is returned to the account it originated from. If you want to return it to another account, you can have a redirection set up.

You can either redirect to another account in your structure, or you can have a “redirection account” set up, this is an account set up specifically for redirections. Speak to your sponsor for more information.

6.3 Allowed transactions and currencies

Accounts in your structure have allowed transactions and currencies set against them. These set the types of transactions and the currency of these transactions (sterling or euro) that you can originate from this account. If you try to originate, for example, a Direct Debit from an account that is not set up to originate Direct Debits, the payment instruction will be rejected.

6.4 Financial limits

Financial limits are set against each account in your account structure. These can be account limits and/or item limits. Credit and debit limits can be set.

These limits are designed to help protect you from errors in the values of payment instructions submitted. If you think a submission will exceed account or item limits, you must discuss this with your sponsor as soon as you can before making the submission. If you exceed your limits, BACS may notify the bank/building society with responsibility for the account; this could impact processing.

If your submission profile changes (that is, the frequency with which you submit and/or the amounts you submit), you need to discuss this with your sponsor so they can set limits they feel are appropriate.

Account limits

Account limits set the total value of credit/debit transactions that can be originated from an account over a specified period: daily, weekly, monthly or a particular number of days (periodic).

In grouped accounts, the account limit is set on the group main account; the value of transactions from all group individual accounts under it are added together for the limit check.

Item limits

Item limits set the limits for individual payment instructions and can be set for credit and/or debit payment instructions for each account in your structure.

Payment instructions that exceed credit or debit item limits are highlighted on your input report; see section 12.1, page 50. If you frequently see these on your input report, you should discuss your limits with your sponsor.

Part III

Your BACSTEL-IP software

❗ *Before using your BACSTEL-IP software to make live submissions, your sponsor links your software to your service user and sets it to live. If the software is not set to live, live submissions* ***will be rejected****.*

To submit via BACSTEL-IP, you need software that is approved under the BACS Approved Software Service for BACSTEL-IP. In this guide, this is referred to as BACSTEL-IP software. This software also allows you to access your reports.

All direct submitters need at least one BACSTEL-IP software package linked to their service user; they can have up to three packages. Before you can use the software to make live submissions, your software must be “live”. This is done after you have completed a series of tests, called a qualification plan; usually your software supplier will help you with these tests.

This part provides an overview of what your software does; for information on how to use your software, please see the documentation provided with it.

Note: If you need to make unattended submissions, this can be done using an HSM (hardware security module). An HSM holds PKI credentials instead of them being held on a smartcard. You need BACSTEL-IP software that supports the use of HSMs. An HSM can only be used with BACSTEL-IP software, it cannot be used on payment services. Please contact your sponsor or solution supplier for more information.

7 Overview of your software

BACSTEL-IP software has been checked to ensure it meets specified standards and provides core functionality for you, including:

- Checks before you send a submission
- Signing your submission
- Establishing a secure connection to BACSTEL-IP
- Submitting and report accessing.

Some service users may create submissions/payment files in a package other than their BACSTEL-IP software. When this is done, you must ensure the submission/payment file is created in the correct format. Your BACSTEL-IP software still performs checks on the submission before you send it.

7.1 Checks before you send a submission

Before you send a submission, your software performs some checks on it. This helps to minimise problems during processing. The checks include:

- Basic structure of the submission and its contents
- Processing dates to ensure they are valid
- Originating account details including allowed transactions
- Destination account details by performing modulus checking
- Destination sorting codes against the Industry Sorting Code Directory (ISCD).

If these checks find any errors, your software details these. You must correct any errors before you send the submission. Warning messages can also be generated during this validation. These are also reported. You must check these warnings carefully and, if necessary, correct any problems. You can still send a submission with warnings.

These checks are only a subset of checks that BACS makes, so problems can still be found during processing. But, the checks help minimise this.

Note: These checks use modulus checking algorithms, the Industry Sorting Code Directory (ISCD) and the BACS processing calendar to validate payment information. Your solution supplier provides you with updates of these. You must upload these into your software when they are available; your solution supplier will tell you how.

7.2 Signing submissions and payment files

All submissions to BACSTEL-IP must be digitally signed using valid PKI credentials. Payment files can also be signed. The person that signs a:

- **Submission** must be a contact for the service user (or bureau) sending the submission
- **Payment file** must be a contact for the service user originating the payments in the file.

In both cases the contact must have a PKI status of active and must have the correct privilege.

Different contacts could sign the payment file and submission. A different contact could also send the submission.

Submissions and payment files should, where possible, be signed on the same day as they are submitted. This avoids problems if PKI credentials expire between the signing being done and the signature being checked.

Your BACSTEL-IP software will guide you through the process of signing submissions and files.

Payment file signatures

As part of your three-day licence details there is a payment file level signature flag. If this flag is set to *yes*, **all your payment files must be digitally signed**. If a file is not properly signed, it will be rejected. For information on how to change this flag, see section 9.1, page 37.

If this flag is set to *no*, payment files can optionally be signed. A signed payment file can be submitted on your behalf by a bureau even if you do not have a relationship set up with the bureau.

7.3 Connecting to BACSTEL-IP

To make submissions or access reports using your software you must connect to BACSTEL-IP. This is normally done via the dial-up extranet or one of a number of “always on connections” but can also be done over the internet (see *Connecting to Bacstel-IP*, page 17). Once connected, you log on to BACSTEL-IP using your PKI credentials. To access reports or send submissions once you are logged on, you must have the correct privilege(s).

You cannot use ASM with BACSTEL-IP software.

When logged on, if there is no activity for 10 minutes your session times out. You have to reauthenticate yourself using your PKI credentials. When you reauthenticate, you continue from where you left off. After four hours of inactivity, however, you are logged off completely.

7.4 Sending a submission

When you send a submission via BACSTEL-IP, checks are made while you are connected. These checks are similar to the presubmission validation performed by your software.

Any errors or warnings generated are displayed to you in your software. All messages should be read carefully and actioned appropriately. The messages include information about the warning/error, what part of the submission caused the problem and what will happen (ie will BACS amend information, is the submission rejected or is it just a warning). Information about who to contact if you are concerned is also included.

When a submission is fully received or is rejected or terminated, a submission summary report is displayed to you. This details the submission received, the payment file(s) in the submission and any errors detected. You should save or print this report for your records. You can also see this information on payment services; see section 13, page 55.

If you send a submission in error, you must contact your sponsor immediately.

Note: Submissions accepted by BACSTEL-IP can still have problems during full validation. You must check your input report to ensure processing by BACS. See section 12.1, page 50 for information about input reports.

7.5 Accessing reports

You can access and download reports using your BACSTEL-IP software. Reports can be downloaded in HTML (as a web page to be viewed, printed and/or saved) or in XML (for local processing). More than one report can be downloaded at a time.

The same reports that can be accessed using your software can be accessed using payment services. Reports are kept for the same amount of time. For information on reports, see part V, starting on page 43.

Notifications can be set up to let you know when new reports are available; see section 8.4, page 34.

7.6 Qualification plan and testing

You can only use software approved under the BACS Approved Software Service for BACSTEL-IP. In addition, your software package needs to be linked to your service user by your sponsor. When this is done, a “qualification plan” is set up for you to complete. This plan is a series of tests.

Normally, your solution supplier helps you with the tests – these will be coordinated with your sponsor. One of your PSCs must complete the following mandatory activities:

- Successfully logging on using PKI
- Accessing the generic test report
- Making a submission that undergoes online validation.

You may also have to make a full live simulation test submission. This generates a test input report that will be checked by your sponsor.

When your qualification plan is complete, your sponsor will set your software status to live. **If your software status is not live, a live submission will be rejected.**

Part IV

Service user information

This part describes the information that you can view and update about your service user on payment services if you have the appropriate privilege (only PSCs can be given these privileges).

Each section shows the menu path you follow to get to the screen beside the ↳ icon (note that after selecting *View service users*, you have to select your service user from a list); it also shows the fields you can see on the screen. Fields in **bold** can be updated by a PSC with the appropriate privilege. The procedure to update the fields is included.

If there is any information displayed that you do not believe is correct and that you cannot update yourself, please contact your sponsor.

8 Service user summary screens

8.1 *Service user details* screen

This screen shows basic information about your service user.

Service users > View service user details > Service user details

Field	Description
Scheme member name / sponsoring bank code	The name of your sponsor and their bank code.
Service user number / name	The name and number of your service user.
Status	This is *Active*.
Service user registration type	This is shown as *BACSTEL-IP*.
Service user type	This is either: • Service user • Bureau. For more information, see section 5.1, page 22.
Registration date	This is the date this service user was first registered on BACSTEL-IP.
Dial-up extranet user	This is *Yes* (you have an extranet ID set up) or *No*.
Extranet ID and password issue date	If dial-up extranet user is *Yes*, these fields are displayed. If you need your password resent or reset, contact your sponsor. For information on the dial-up extranet, see the *Contact's guide*, section 24, page 80.
Email address	This is the default email address for your service user. It may be used by BACS to send notifications and by your sponsor to contact you. You must make sure it is kept up to date. This can be up to 50 characters.
Address details	This is your service user's address. You must make sure it is kept up to date.
VAT registration number and company registration number	This information is not always recorded. If it is, and it is wrong, contact your sponsor.

8.1.1 Maintaining your postal and email address

Your default email address and postal address can be updated. If you are a Direct Debit originator, you may also need to change your DDO email and postal address details; see section 9.3, page 39.

To maintain your postal and email address

You must be logged on to payment services with ASM or PKI, and have the relevant privilege.

1 Select *Service users > Maintain service user details*

From the main menu, select *Service users*. Then click *Maintain service user details* on the *Service users menu* screen and select the service user you want by clicking on the service user number. The *Service user maintain summary* screen loads.

2 Select *Service user details including marketing data*

In the *Service user details* row, click *maintain*. The *Service user details* screen loads.

3 Make the required changes

You can change the default email address and/or the address details. The email address can be up to 50 characters and is mandatory. The address details are made up of:

- Addressee name (up to 33 characters, mandatory field)
- Postal name (33 characters, mandatory)
- Address line 1 and 2 (33 characters each)
- City/town (30 characters)
- County (24 characters)
- Post code (2 fields, 4 and 3 characters)
- Country (selected from a drop down).

When you are done, click *submit*. The *Service user details summary* screen loads.

4 Check the summary and confirm using security credentials

Check the summary. If it is correct click *confirm*. The *Security check* screen loads:

- **If you are logged on with PKI,** your signing software opens. With your smartcard in the reader, use your PIN to sign the information
- **If you are logged on with ASM,** enter your password and click *OK*.

If successful, the *Success* screen loads.

8.2 *Organisations* screen

This screen shows the organisation your service user is linked to.

Service users > *View service user details* > *Service user organisations*

Field	Description
Organisation name / ID	The name of the organisation you are linked to. (The organisation ID is a unique identifier for this organisation.)
Head office indicator	When an organisation contains multiple service users, this flag shows if your service user is the head office.

8.3 *Trading names* screen

This screen shows trading names associated with your service user. Trading names are only normally recorded if you originate Direct Debits.

Service users > *View service user details* > *Service user trading names*

Field	Description
Trading name	If your service user trades under a trading name.
Status	Indicates if this trading name is *Current*, *Withdrawn* or *Deleted*.
Registration date	The date this trading name was registered.

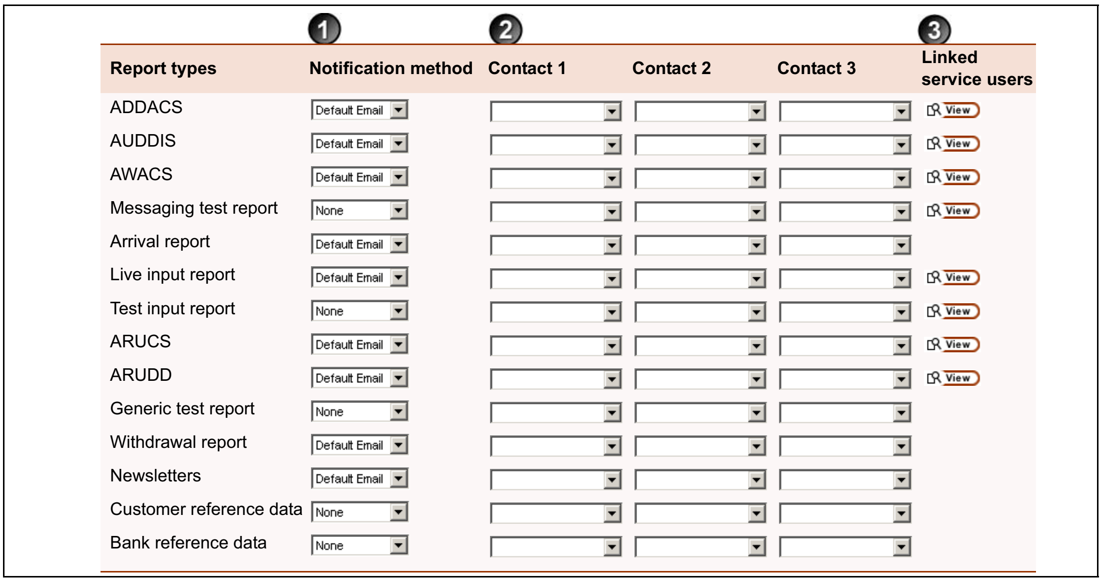
8.4 *Notifications* screen

This screen shows details of notifications that are set up for your service user when processing and messaging reports are available. The screenshot below shows the contents of this screen. You can update which contacts receive notifications. Bureaux can click on the *view* button to see which (if any) service users they are set up to access reports on behalf of. This returns the *Bureau – linked service users* screen. (If a bureau is set up to access a particular report for a service user, they receive an email notification when one is available if they are set to receive notifications for that report type.)

If a contact is set to receive notifications, contacts must have at least one status (ASM or PKI) set to active; for information on contact statuses see section 14.1, page 59.

If a contact is set to receive notifications for a particular report type, and their status(es) subsequently change to pending or suspended, they will not receive notifications and their name will not be displayed on the notifications screen. If their status goes back to active, they will again receive the notifications they were set up for.

Service users > View service user details > Notifications



Report types	Notification method	Contact 1	Contact 2	Contact 3	Linked service users
ADDACS	Default Email				View
AUDDIS	Default Email				View
AWACS	Default Email				View
Messaging test report	None				View
Arrival report	Default Email				
Live input report	Default Email				View
Test input report	None				View
ARUCS	Default Email				View
ARUDD	Default Email				View
Generic test report	None				
Withdrawal report	Default Email				
Newsletters	Default Email				
Customer reference data	None				
Bank reference data	None				

Figure 4: The Notifications *screen*

Details

1
- **Default email** – notifications go to your default email address, set on the *Service user details* screen
- **Contact email** – you need to select contacts to receive the notification; up to three can be selected
- **None** – you do not get any email notifications for these report types.

2 If the notification method is contact email, select up to three contacts using the drop downs.

3 This section is only displayed for bureaux.

Click *view* to see the service user numbers of service users that you are set up to access reports on behalf of. The button is only displayed against the report types that this function is available to. For more information on bureau collection, see section 10.3, page 45.

8.4.1 Maintaining your notifications

To maintain your notifications

You must be logged on to payment services with ASM or PKI, and have the relevant privilege.

1 Select *Service users* > *Maintain service user details*

From the main menu, select *Service users*. Then click *Maintain service user details* on the *Service users menu* screen and select the service user you want by clicking on the service user number. The *Service user maintain summary* screen loads.

2 Select *Notifications*

In the *Maintain notifications* row, click *maintain*. The *Service user notifications* screen loads.

3 Make the required changes

For any report types that have a notification method of contact email, you can select the contacts to receive a notification. Up to three can be selected for each report type. (To change which reports generate notifications, contact your sponsor.) When you are done, click *submit*. The *Service user notifications summary* screen loads.

4 Check the summary and confirm using security credentials

Check the summary. If it is correct click *confirm*. The *Security check* screen loads:

- **If you are logged on with PKI,** your signing software opens. With your smartcard in the reader, use your PIN to sign the information
- **If you are logged on with ASM,** enter your password and click *OK*.

If successful, the *Success* screen loads.

8.5 Contact list screen

This screen lets you see the contacts linked to your service user. You cannot maintain contacts from this screen.

Service users > *View service user details* > *View contacts*

Column	Description
Contact ID	The contact ID of the contact
First name / last name	The first and last name of the contact.
Contact type	Whether the contact is a PSC (primary security contact) or AC (additional contact).

9 Three-day service licence screens

9.1 *Three-day licence details* screen

This screen shows general information about your three-day licence.

Service users > View service user details > BACS three-day licence > Licence details

Field	Description
User role	This is either *Direct* or *Indirect* submitter. For more information, see section 5.2, page 22.
User grade	This indicates if you are: • Customer grade – most service users are set to this • Government grade • Bank grade.
Licence start date	The date your three-day licence was set up.
File level signature	This indicates if payment files submitted by you (or by a bureau on your behalf) have to be digitally signed. If this is set to *yes*, and a payment file is received for your service user number that is not digitally signed, it will be rejected. For more information, see section 7.2, page 27. *Note: You need to be logged on with PKI to change this.*
Status	Three statuses are shown: • Authentication – this is set to *no* • Telecoms – this may be *Live*, *Test* or *No*. To submit live files via BACSTEL-IP it must be *Live* • HST – if you submit over the HST input channel, this is set to *Live* or *Test*, otherwise it is set to *No*.

9.1.1 Maintaining your file level signature flag

> *Note: If you set your file level signature flag to “yes”,* ***all*** *payment files originated by your service user must be digitally signed,* ***or they will be rejected****.*
>
> *(The payment file must be signed by a contact with the appropriate privilege that is associated with the service user that originated the payments in the file.)*

To maintain your file level signature flag

You must be logged on to payment services with PKI, and have the relevant privilege.

1 Select *Service users > Maintain service user details*

From the main menu, select *Service users*. Then click *Maintain service user details* on the *Service users menu* screen and select the service user you want by clicking on the service user number. The *Service user maintain summary* screen loads.

2 Select *BACS three-day licence > Licence details*

In the *BACS three-day licence* row, click *maintain*. Then click *maintain* in the *Licence details* row. The *Service user three-day licence details* screen loads.

3 Set the file level signature flag

In the *File level signature flag* drop down, select *yes* to indicate that file level signatures are needed, or *no* if they are not.

If *yes* is set, any payment file received for your service user that is not digitally signed will be rejected. If *no* is set, payment files do not have to be signed (however, they will be accepted if they are signed correctly).

Click *submit*. The *Service user licence details summary* screen loads.

4 Check the summary and confirm using security credentials

Check the summary. If it is correct click *confirm*. The *Security check* screen loads. With your smartcard in the reader, use your PIN to sign the information. If successful, the *Success* screen loads.

9.2 *Accounts list* screen

This screen shows the account numbers and sorting codes of accounts in your account structure. The screen is split in two sections:

- Owning accounts – those that are held with your sponsor
- Nonowning accounts – those held at a bank/building society other than your sponsor.

For general information about accounts, see section 6, page 23.

Service users > View service user details > BACS three-day licence > Account details

Field	Description
Account number / sorting code	The details of the account.
Type	This is current or deposit, depending on the type of account.
Group main code	This is shown for group main and group individual accounts. It is a letter showing you the group individual accounts that are linked to the group main account.
Account type	This shows if the account is a: • Main account • Individual account • Group main account; or • Group individual account.

These details are repeated for each account in your structure.

9.3 *DDO details* screen

You can only see this screen if your service user is set up to originate Direct Debits.

This information may be used by banks/building societies if they need to contact you regarding a Direct Debit or a Direct Debit Instruction (DDI) that has originated from your service user. The user administration contact (if one is listed) would normally be contacted in the first instance. This should be the person that could answer day to day queries.

Service users > View service user details > BACS three-day licence > DDO details

Field	Description
Scheme contact details	Contains name, address and telephone numbers. For information on the fields, see the update procedure.
User administration details	Contains name, address and telephone numbers. For information on the fields, see the update procedure.

9.3.1 Maintaining your DDO details

If you change these address details, you should also check your main service user address details to ensure they are correct; see section 8.1, page 32.

To maintain your service user details

You must be logged on to payment services with ASM or PKI, and have the relevant privilege.

1 Select *Service users > Maintain service user details*

From the main menu, select *Service users*. Then click *Maintain service user details* on the *Service users menu* screen and select the service user you want by clicking on the service user number. The *Service user maintain summary* screen loads.

2 Select *BACS three-day licence > DDO details*

In the *BACS three-day licence* row, click *maintain*. Then click *maintain* in the *DDO details* row. The *Service user – DDO details* screen loads.

3 Make the required changes

Scheme contact details are mandatory (as detailed in the list below); user administration details are optional (except email and telephone, which are mandatory), but if you enter an addressee name and postal name, you must also enter address line 1, city/town, and country:

- Addressee name, postal name (up to 33 characters each, mandatory fields)
- Address line 1 and 2 (33 characters each)
- City/town (30 characters)
- County (24 characters)
- Post code (2 fields, 4 and 3 characters)
- Country (selected from a drop down)
- Email address (50 characters), fax number (5 and 10), telephone number (5 and 10); email and telephone are mandatory.

When you are done, click *submit*. The *Service user DDO details summary* screen loads.

4 Check the summary and confirm using security credentials

Check the summary. If it is correct click *confirm*. The *Security check* screen loads:

- **If you are logged on with PKI,** your signing software opens. With your smartcard in the reader, use your PIN to sign the information
- **If you are logged on with ASM,** enter your password and click *OK*.

If successful, the *Success* screen loads.

9.4 Software packages

These screens show details of your BACSTEL-IP software. They also show details of the qualification plan outlining the testing needed before your software is set to live.

Software packages list screen

Service users > View service user details > BACS three-day licence > Software packages and qualification plans

Field	Description
Package name and version	The name and version number of the software package.
Status	This is the status of the qualification plan, *live* or *test*. To send live submissions using this package, it must be live, otherwise the submission will be rejected.
Solution supplier	The name of the solution supplier for this package.

9.5 *Bureau details* screen

This screen shows you details of bureaux authorised to submit on your behalf. It is only shown for service users; bureaux do not see this screen.

Service users > View service user details > BACS three-day licence > Bureaux details

Field	Description
Bureau number / name	The number of the bureau; the name of the bureau.
Sponsor name	The name of the scheme member that sponsors the bureau.

Bureau report access screen

From the *Bureau details* screen, click *bureau report access* to see bureau that are set up to access your reports. This screen lists bureaux linked to your service user across the top, and report types on the left. If a bureau is set up to access a particular report type, a tick is displayed.

Part V
Reports and submissions

This part describes how you can use payment services to view processing and messaging reports and view information about your submissions. It also describes the different reports you may receive.

If you are using your BACSTEL-IP software to get reports, see documentation that came with your software for information on how to access reports.

If your payment file has been submitted by a bureau using the BACSTEL® service, you can still view your reports on payment services. You can only view submissions if you are linked to the service user or bureau that made the submission.

In addition to the reports in this section, a submission summary report is sent to your BACSTEL-IP software when a submission is sent. This tells you if it was accepted and provides a list of warnings or errors detected.

Some bureau may offer a service to collect reports on your behalf from payment services. Your sponsor needs to set up permissions to allow a bureau to do this.

> *Note: It is essential that you check all reports produced. They contain important information about the processing of your payments.*
>
> *When you receive messaging reports, you should make the necessary updates to your database to ensure future payments are addressed correctly.*
>
> *If you have any concerns about the contents of your reports, speak to your sponsor.*

10 Reports – overview

Reports generated following a submission are accessed using payment services or your BACSTEL-IP software. You also normally receive your messaging reports on BACSTEL-IP.

The table below lists the reports available and the section to see for more information on them.

Processing reports	Information
Input reports (live and test)	Sec 12.1, pg 50
Withdrawal reports	Sec 12.2, pg 51
Arrival reports	Sec 12.3, pg 52
ARUCS (automated return of unapplied credits service) reports	Sec 12.4, pg 52
ARUDD (automated return of unpaid Direct Debits) reports	Sec 12.4, pg 52
AUDDIS (Automated Direct Debit Instruction Service)	Sec 12.5, pg 53
ADDACS (Automated Direct Debit and Cancellation Service)	Sec 12.6, pg 53
AWACS (advice of wrong account for automated credits service)	Sec 12.7, pg 53

As well as these reports, a generic test report and messaging test reports are available; use these to make sure you can access reports OK.

When reports are available, you can receive email notifications. This notification can be to a default email address or as many as three contacts. For information on viewing and updating notifications, see section 8.4, page 34.

10.1 Report formats

Reports can be viewed in HTML (as a regular web page) or downloaded as HTML or XML. XML provides the report unformatted allowing the data to be uploaded into another application. You need appropriate software to use XML reports this way.

When you view a report (in HTML), only the first 30 pages are displayed. However, most reports are only a few pages so this does not cause any problems. If a report is more than 30 pages, a message is included on the last page saying it has been truncated. To see the entire report download it in HTML (rather than just viewing it), or, if it is an ARUCS or ARUDD report, a compact version can be viewed. This report has the same information but less page breaks. The procedure to access reports tells you how to do this.

When you download more than one report on payment services, the reports are put in a zip file. This file is not compressed, but the zip file is used to group the reports and associated files. So if you download more than one report you need WinZip or similar software. Windows XP allows access to zip files without any additional software.

10.2 Report availability

You should always access your reports promptly when they are available – make sure you have appropriate notifications set up so you know when reports are ready; see section 8.4, page 34.

Accessing a report does not remove it from BACSTEL-IP. However, reports are only available on payment services and through your software for a set period. This period is configurable and may change. Currently, you should always have access to at least:

- The last 10 reports generated for your service user
- All reports generated for your service user in the past 6 days.

10.3 Bureau access of reports

Bureaux can be set up to access reports on behalf of a service user that they are linked to (the sponsor of the service user sets up the link and sets the access permissions for the bureau to get reports). Up to five bureau can be given permission to access reports for a service user. Permissions can be given for the following report types:

- Input reports (only the bureau that sent the submission can view the report)
- ARUCS reports
- ADDACS reports
- AWACS reports
- Test input reports (only the bureau that sent the submission can view the report)
- ARUDD reports
- AUDDIS reports
- Messaging test reports

Arrival reports are automatically made available to the submitter as normal. A version of the withdrawal report is created for the submitting bureau as normal.

Accessed flags

There are two system settings that record if a report has been accessed: one for a bureau contact accessing it and one for a service user contact accessing it (the flag is set whether the report is accessed using payment services or your BACSTEL-IP software). The settings are used by the system when you perform a report search. If you are a contact associated with a:

- **Bureau** and search for unaccessed reports, you get reports not accessed by a bureau contact; reports accessed only by a service user contact are found in the search
- **Service user** and search for unaccessed reports, you get reports not accessed by a service user contact; reports accessed only by a bureau contact are found.

If you are a contact linked to a service user and a bureau, when you access reports, the system records this as a service user accessing the reports. So if you search for unaccessed reports, you see reports not accessed by a service user contact.

When a service user contact accesses a report, the accessed flag displayed on-screen is updated to show that the report has been viewed (this flag is seen by all contacts). (This means if a bureau contact searches for, for example, unaccessed reports, some may have accessed dates listed on screen.)

Viewing bureau report permissions

Bureau can see the service users that they can access reports for, and service users can see the bureaux set up to access their reports. Only the sponsor of the service user can maintain these settings:

- **Bureau** can see details from the *Notifications* screen, see section 8.4, page 34
- **Service users** can see details from the *Bureau details* screen, see section 9.5, page 41.

10.4 Print settings

To make sure your reports fit on the page when you print, you may have to change some settings. Page orientation and margins normally need to be changed each time you print.

Type	Setting
Page orientation	Must be landscape. This is normally set in your browser by selecting *File*, *Page setup*. In *Orientation*, select *Landscape*.
Margins	You may need to reduce your margins so the report does not get cut off on the edges. In your browser, select *File*, *Page setup*. Suggested margin sizes are: • Left and right margins of 16 mm • Top and bottom margins of 19.05 mm. If these do not work, alter the margins further.
Text size	The text size in your browser should be set to “medium”. Select *View, Text size, Medium*.
Font	You must have at least one of the following fonts installed on your computer: Lucida Console, Andale Mono or Courier New.

11 Accessing reports on payment services

To access reports

You must be logged on to payment services with ASM or PKI, and have the relevant privilege.

1 Select *Processing reports*

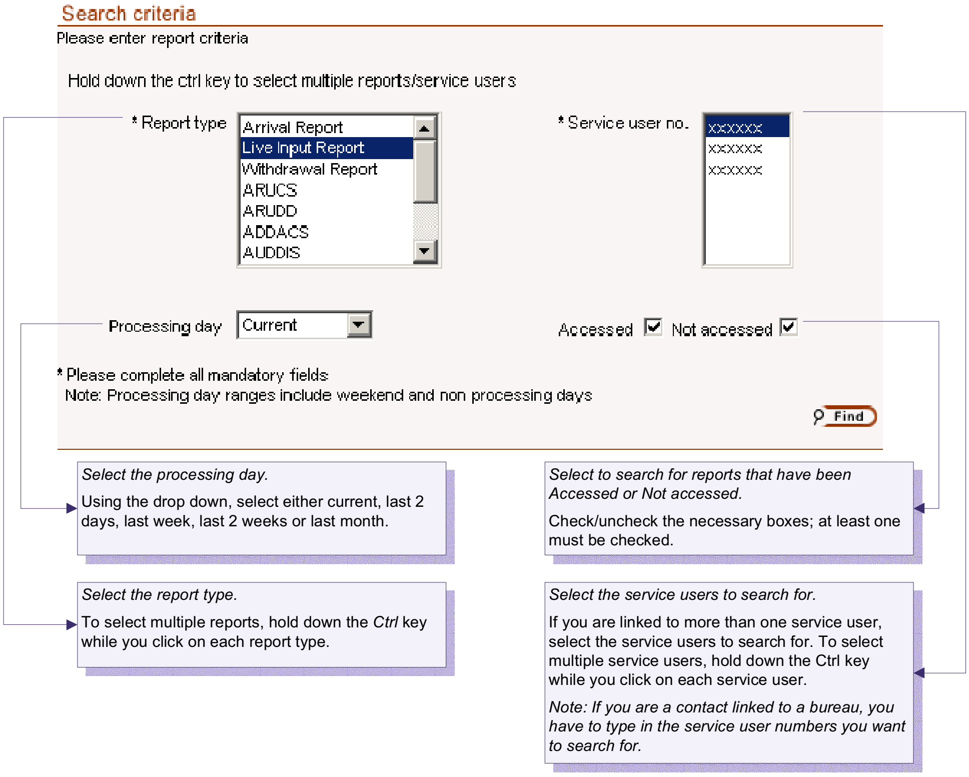
From the main menu, select *Processing reports*.

If you are linked to more than one service user or you are linked to a bureau, the *Processing reports search* screen loads (go to the next step).

If you are linked to only one service user, you get a list of reports available (go to step 3); you can reduce the number shown by clicking search (go to the next step).

2 Search for the reports you need

Enter the following information to search for reports.



Search criteria

Please enter report criteria

Hold down the ctrl key to select multiple reports/service users

* Report type: Arrival Report, Live Input Report (selected), Withdrawal Report, ARUCS, ARUDD, ADDACS, AUDDIS

* Service user no.: xxxxxx (selected), xxxxxx, xxxxxx

Processing day: Current

Accessed ☑ Not accessed ☑

* Please complete all mandatory fields
Note: Processing day ranges include weekend and non processing days

Select the processing day.

Using the drop down, select either current, last 2 days, last week, last 2 weeks or last month.

Select to search for reports that have been Accessed or Not accessed.

Check/uncheck the necessary boxes; at least one must be checked.

Select the report type.

To select multiple reports, hold down the *Ctrl* key while you click on each report type.

Select the service users to search for.

If you are linked to more than one service user, select the service users to search for. To select multiple service users, hold down the Ctrl key while you click on each service user.

Note: If you are a contact linked to a bureau, you have to type in the service user numbers you want to search for.

Click *find*. If reports (that you have the privilege to view) match the search, the *Processing reports* screen loads. Otherwise this screen reloads with an error.

Note: The generic test reports and messaging test reports have no processing day and no accessed/nonaccessed flag associated with them. This means, if either of these report types are selected, the report is always returned, regardless of other search criteria.

To access reports (continued)

3 View or download your reports

On the *Reports* screen, to view other reports, or reduce the number of reports displayed, click *search*; go to step 2.

The list shows details of the report including its date, the file size (if accessed in HTML) and, if it has been accessed, the contact ID of the first service user contact to access it is displayed; for more information on this setting, see section 10.3, page 45.

To view a report (in HTML), click the 🗎 icon beside the report you want. For ARUCS and ARUDD reports, you can view a compact version by clicking the 🗐 icon. A new browser window opens displaying the report.

To save or print the report, select the *File* menu and *Print* or *Save*. To print correctly, you may have to change some of your browser settings, see section 10.4, page 46.

When finished with the report, close the browser window it opened in.

To download multiple reports, select the *Download type*, HTML or XML. Then either:

- Click *download all*, this downloads all reports listed on the page; or
- Select the reports to download by checking the appropriate boxes (the reports selected must all be on the same page). Click *download.* (To download one report in HTML, you should view the report and then save it.)

A dialogue box normally opens with the option to open or save the file (some web browsers may be set to automatically open or save the file). Select either option:

- If save is chosen, select the location to save the zip file
- If open is selected, the computer's zip software (eg WinZip) opens and the file downloaded is displayed.

To open reports downloaded as zip files, see section 11.1, page 49.

11.1 Opening zip files

This section provides general advice on opening zip files using WinZip and using Windows XP, which comes with its own compression software. For additional help, please consult your own IT staff or documentation that came with your zip software or operating system.

To open a zip file using WinZip

You must have downloaded multiple reports and have WinZip installed.

1 Open the zip file

If you chose to save the zip file, locate it using Windows Explorer and open it. WinZip should automatically open. If you chose to open the zip file, WinZip should already be open.

2 Extract the files

In the WinZip toolbar, click *Extract*. The *Extract* dialogue opens.

3 Select when to save the files

In the *Folders/drives* field, select the folder to save the files to by clicking it once with your mouse; this highlights the folder. (Drives and folders can be expanded by clicking the ⊞ symbol beside them.)

The *Extract* dialogue closes and WinZip extracts the file. The status bar at the bottom of the WinZip window displays a message indicating it is extracting files. The reports are extracted to the selected folder. If the reports are in HTML, a folder called *stylesheets* is also saved; this contains images used to display reports properly.

To open a zip file using Windows XP

You must have downloaded multiple reports and be using Windows XP.

1 Open *My Computer*

Click *Start*, *My computer*. Find the file you saved (it is usually displayed as a folder icon with a zipper on it).

2 Extract the file

Right click on the file and select *Extract all*. The *Compressed folders extraction wizard* opens. Follow the instructions to extract the files.

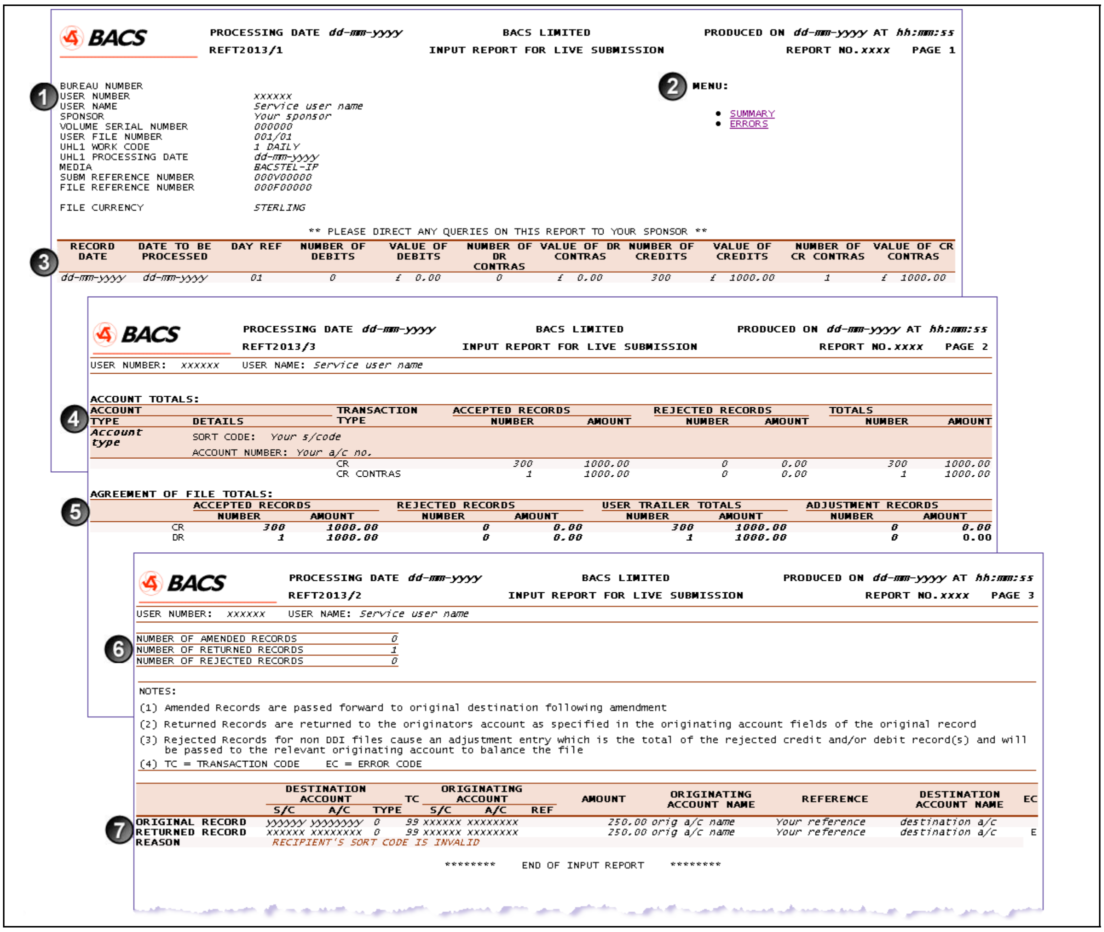
12 About the reports

This section provides an overview of the reports that can be accessed. For a summary of when the reports are produced during processing, see the table on page 14.

12.1 Input reports

Input reports are produced by the BACS service after a day section has been successfully validated on input day. It is usually available about four hours after a day section has been validated. If your file contained Direct Debit Instructions, you get a separate input report for these. On the report, the total of DDIs appears in the number of debits column; other fields are set to zero.

The report must be checked as it confirms that your information has been processed by BACS. Your input report highlights any payment instructions amended, rejected or returned by BACS. If a payment is rejected or returned, you should take the necessary action to ensure any errors are corrected and resubmit the payment if needed. Please note, some payment instructions could still be returned by the receiving bank or building society.



BACS PROCESSING DATE *dd-mm-yyyy* BACS LIMITED PRODUCED ON *dd-mm-yyyy* AT *hh:mm:ss*
REFT2013/1 INPUT REPORT FOR LIVE SUBMISSION REPORT NO.*xxxx* PAGE 1

BUREAU NUMBER	
USER NUMBER	*xxxxxx*
USER NAME	*Service user name*
SPONSOR	*Your sponsor*
VOLUME SERIAL NUMBER	*000000*
USER FILE NUMBER	*001/01*
UHL1 WORK CODE	*1 DAILY*
UHL1 PROCESSING DATE	*dd-mm-yyyy*
MEDIA	*BACSTEL-IP*
SUBM REFERENCE NUMBER	*000V00000*
FILE REFERENCE NUMBER	*000F00000*
FILE CURRENCY	*STERLING*

MENU:

- SUMMARY
- ERRORS

** PLEASE DIRECT ANY QUERIES ON THIS REPORT TO YOUR SPONSOR **

RECORD DATE	DATE TO BE PROCESSED	DAY REF	NUMBER OF DEBITS	VALUE OF DEBITS	NUMBER OF DR CONTRAS	VALUE OF DR CONTRAS	NUMBER OF CREDITS	VALUE OF CREDITS	NUMBER OF CR CONTRAS	VALUE OF CR CONTRAS
dd-mm-yyyy	*dd-mm-yyyy*	*01*	*0*	*£ 0.00*	*0*	*£ 0.00*	*300*	*£ 1000.00*	*1*	*£ 1000.00*

BACS PROCESSING DATE *dd-mm-yyyy* BACS LIMITED PRODUCED ON *dd-mm-yyyy* AT *hh:mm:ss*
REFT2013/3 INPUT REPORT FOR LIVE SUBMISSION REPORT NO.*xxxx* PAGE 2
USER NUMBER: *xxxxxx* USER NAME: *Service user name*

ACCOUNT TOTALS:

ACCOUNT		TRANSACTION	ACCEPTED RECORDS		REJECTED RECORDS		TOTALS	
TYPE	DETAILS	TYPE	NUMBER	AMOUNT	NUMBER	AMOUNT	NUMBER	AMOUNT
Account type	SORT CODE: *Your s/code* ACCOUNT NUMBER: *Your a/c no.*							
		CR	*300*	*1000.00*	*0*	*0.00*	*300*	*1000.00*
		CR CONTRAS	*1*	*1000.00*	*0*	*0.00*	*1*	*1000.00*

AGREEMENT OF FILE TOTALS:

	ACCEPTED RECORDS		REJECTED RECORDS		USER TRAILER TOTALS		ADJUSTMENT RECORDS	
	NUMBER	AMOUNT	NUMBER	AMOUNT	NUMBER	AMOUNT	NUMBER	AMOUNT
CR	***300***	***1000.00***	***0***	***0.00***	***300***	***1000.00***	***0***	***0.00***
DR	***1***	***1000.00***	***0***	***0.00***	***1***	***1000.00***	***0***	**0.00**

BACS PROCESSING DATE *dd-mm-yyyy* BACS LIMITED PRODUCED ON *dd-mm-yyyy* AT *hh:mm:ss*
REFT2013/2 INPUT REPORT FOR LIVE SUBMISSION REPORT NO.*xxxx* PAGE 3
USER NUMBER: *xxxxxx* USER NAME: *Service user name*

NUMBER OF AMENDED RECORDS	*0*
NUMBER OF RETURNED RECORDS	*1*
NUMBER OF REJECTED RECORDS	*0*

NOTES:
(1) Amended Records are passed forward to original destination following amendment
(2) Returned Records are returned to the originators account as specified in the originating account fields of the original record
(3) Rejected Records for non DDI files cause an adjustment entry which is the total of the rejected credit and/or debit record(s) and will be passed to the relevant originating account to balance the file
(4) TC = TRANSACTION CODE EC = ERROR CODE

	DESTINATION ACCOUNT			TC	ORIGINATING ACCOUNT			AMOUNT	ORIGINATING ACCOUNT NAME	REFERENCE	DESTINATION ACCOUNT NAME	EC
	S/C	A/C	TYPE		S/C	A/C	REF					
ORIGINAL RECORD	*yyyyyy*	*yyyyyyyy*	*0*	*99*	*xxxxxx*	*xxxxxxxx*		*250.00*	*orig a/c name*	*Your reference*	*destination a/c*	
RETURNED RECORD	*xxxxxx*	*xxxxxxxx*	*0*	*99*	*xxxxxx*	*xxxxxxxx*		*250.00*	*orig a/c name*	*Your reference*	*destination a/c*	E
REASON	*RECIPIENT'S SORT CODE IS INVALID*											

******** END OF INPUT REPORT ********

Figure 5: An example of an input report

	Details
1	This shows basic information to help you identify the payment file that the day section was in. Information includes: • *Bureau number* of the bureau that submitted the file. This is blank if the user submitted directly • *UHL1 workcode* is 1 DAILY for single processing day files or 4 MULTI for multiprocessing day files • *UHL1 processing date* is the processing date of the file • *File currency* is euro or sterling.
2	These hyperlinks only appear when you view the report online. The error link appears even if there are no errors listed in the report.
3	This provides details of the day section that has been processed by Bacs and are included on this input report. Normally, only one line is displayed. More than one line appears if an invalid processing date was used and therefore overridden by Bacs and this overridden date matches that of another day section in the payment file. Two dates are shown on each line: • *Record date* is the original processing date of the day section • *Date to be processed* is the date the day section is going to be processed on (this is the same as the record date unless an invalid processing date was used).
4	This provides a break down of the account sections processed. The originating sorting code and account number are shown with the totals of accepted and rejected records (payment instructions).
5	This shows the file totals in the day section, showing the values of accepted and rejected records. Also shown are the user trailer totals (the total value of the payment file) and any adjustment records generated by Bacs. Adjustment records are generated if payment instructions are rejected; this ensures that a day section still balances even if a payment instruction is rejected.
6	This is a break down of the total number of amended, returned and rejected payment instructions.
7	This shows details of payment instructions that are amended, returned and/or rejected and the reasons why. Any highlighted or audit payment instructions are also shown.

12.2 Withdrawal reports

If a payment file is submitted in error you can contact your sponsor on or before input day to request an extraction. When an extraction is carried out, a withdrawal report is generated.

The report shows whether the extraction was done at submission, payment file or day section level. If a submission was made by a bureau, both the bureau and the affected service user receive a copy of the withdrawal report.

You should check withdrawal reports to ensure the required data was extracted.

12.3 Arrival reports

There are two types of arrival reports: rejection arrival reports and acceptance arrival reports. A rejection arrival report is produced in the following cases:

- A submission is rejected during arrival day validation (for example, if BACS detects that a service user has submitted the same file twice for the same processing day)
- A bureau submission contains a payment file for an unrecognised service user.

An acceptance arrival report is produced in the following case:

- A HST submission with at least one day section that is future dated.

12.4 ARUCS and ARUDD reports

If you submit a payment instruction that passes BACS validation but cannot be applied by the destination bank or building society, those payment instructions are returned to your originating account. For example, if you try to make a payment to someone that has closed their account, the bank/building society returns the money to you.

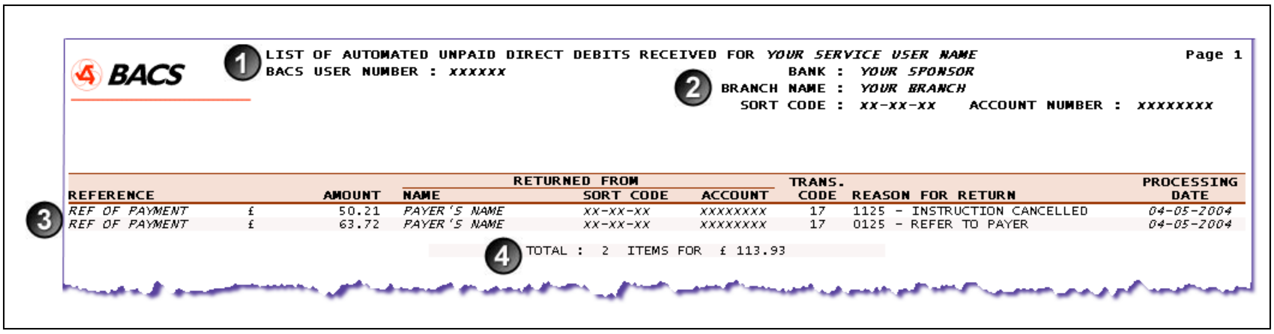
This functionality is provided by two services, depending on whether it is a credit or debit:

- ARUCS – automated return of unapplied credits service
- ARUDD – automated return of unpaid Direct Debits.

Both services produce advices that are compiled into reports. These reports list the payments that could not be applied and the reason. You should update your records accordingly.

The payment is normally applied to your originating account on the next valid processing day after the date of the report.

The following figure is an example of an ARUDD report – the information highlighted on this report is also on an ARUCS report.



```
BACS          LIST OF AUTOMATED UNPAID DIRECT DEBITS RECEIVED FOR YOUR SERVICE USER NAME                          Page 1
              BACS USER NUMBER : XXXXXX
                                                              BANK : YOUR SPONSOR
                                                       BRANCH NAME : YOUR BRANCH
                                                         SORT CODE : XX-XX-XX     ACCOUNT NUMBER : XXXXXXXX

                                               RETURNED FROM                   TRANS.                                 PROCESSING
REFERENCE                  AMOUNT  NAME               SORT CODE   ACCOUNT      CODE   REASON FOR RETURN                    DATE
REF OF PAYMENT      £       50.21  PAYER'S NAME       XX-XX-XX    XXXXXXXX      17    1125 - INSTRUCTION CANCELLED     04-05-2004
REF OF PAYMENT      £       63.72  PAYER'S NAME       XX-XX-XX    XXXXXXXX      17    0125 - REFER TO PAYER            04-05-2004

                                          TOTAL :  2  ITEMS FOR  £ 113.93
```

Figure 6: An example of an ARUDD report

	Details
1	This shows the report name and your service user name and number.
2	This shows the account details of where the returned payment instructions will be applied (this will be the originating account of the original payment instruction).
3	This shows details of the payment instructions that have been returned (processing date is only shown on ARUDD reports). The reason for return shows differently on the two reports: • On ARUDD reports, it shows as four numbers – in the format *RDDD*, *R* is the reason code, *DDD* is the Julian date of the original payment instruction. The text of the reason code is also displayed • On ARUCS reports, the reason code and the text of the reason is displayed. For a list of reason codes, see section 12.8, page 53.
4	This shows the number and value of payment instructions returned to the account detailed in 2 above.

12.5 AUDDIS reports

The advice of bank returned Direct Debit Instructions (AUDDIS) report, part of the AUDDIS service, details DDIs that could not be applied by the recipient bank/building society. You should make any necessary amendments and resubmit the DDI where needed. It also includes DDIs that have been applied after being amended by the recipient bank/building society. You should make any necessary changes to the DDI (you may need to check with the payer) and resubmit the amended DDI.

12.6 ADDACS reports

ADDACS (Advice of Direct Debit Amendments and Cancellation Service) reports detail any Direct Debits that have been amended or cancelled by the payer. When a payer amends or cancels a Direct Debit with their bank, the bank can use the ADDACS service to notify you. The information is sent to BACS who compiles this report for you. You should amend the details you use to collect the Direct Debit in line with the details in the report.

12.7 AWACS reports

AWACS (advice of wrong account for automated credits service) reports detail credit payments that you have originated where the destination details where not correct, but that could still be applied by the recipient bank/building society. You should update your records as detailed in the report to ensure future payments are not subject to delay or rejection.

12.8 Advice reasons

The ARUCS, ARUDD, AUDDIS, ADDACS and AWACS reports all contain reason codes to identify why a payment instruction could not be applied or to provide information on why account details have to be changed. The table following shows the codes used and what they mean for the different services. The explanation of these codes also appears on the reports.

Code	Report				
	ARUCS	ARUDD	AUDDIS	ADDACS	AWACS
0	Invalid details	Refer to payer		Instruction cancelled – refer to payer	Invalid details
1		Instruction cancelled	Instruction cancelled by payer	Instruction cancelled by payer	
2	Beneficiary deceased	Payer deceased	Payer deceased	Payer deceased	
3	Account transferred	Account transferred	Account transferred to another bank	Account transferred to a new bank or building society	Account transferred
4		Advance notice disputed			
5	No account	No account	No account		
6		No instruction	No instruction		
7		Amount differs			
8		Amount not due			
9		Presentation overdue			
A		Originator differs			
B	Account closed	Account closed	Account closed	Account closed	
C	Requested by originator		Account transferred to a different account/branch of the bank/building society	Account/instruction transferred to a different branch of a bank/building society	
D				Advance notice disputed	
E				Instruction amended	
F			Invalid account type		
G			Bank will not accept Direct Debits on account		
H			Instruction expired		
I			Payer reference not unique		
K			Instruction cancelled by bank		

13 Submissions

You can view information about recent submissions made via BACSTEL-IP. Only a contact associated with the service user or bureau that **sent** a submission can see details of it. This means indirect submitters cannot view information in this way.

You can see basic information including the contact that sent the submission as well as any errors or warnings that were generated when the submission was received. These errors and warnings would have been returned to your BACSTEL-IP software when the submission was made.

To view submission information

You must be logged on with PKI to view live submissions (for test submissions you can be logged on with ASM or PKI), and have the relevant privilege.

1 Select *Submissions*

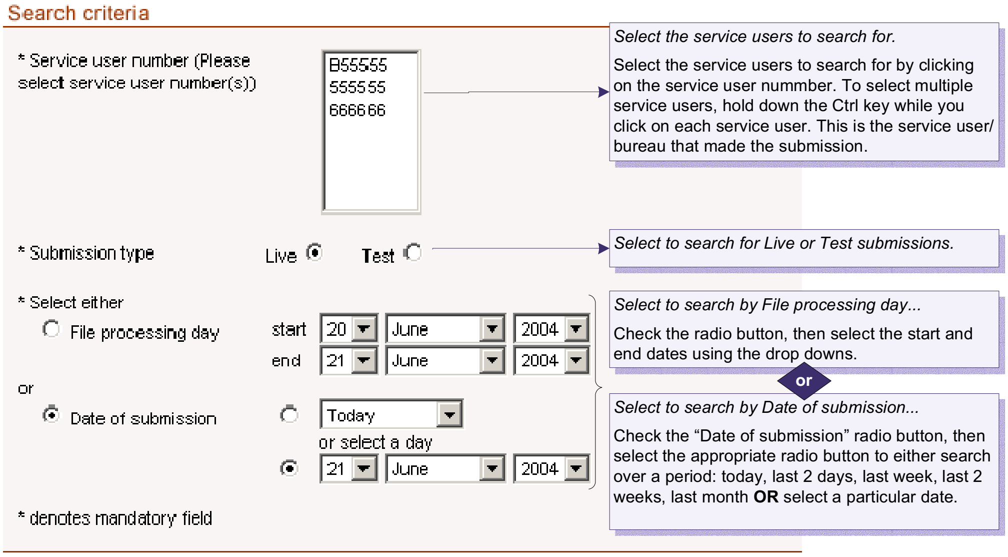
From the main menu, select *Submissions*.

If you are linked to more than one service user, the *Submission search* screen loads; go to the next step.

If you are linked to only one service user, the *Submissions* screen loads; go to step 3.

2 Search for the submissions you need

Search for the submissions.



Search criteria

* Service user number (Please select service user number(s))
B55555
555555
666666

* Submission type Live ● Test ○

* Select either
○ File processing day start 20 June 2004
end 21 June 2004
or
● Date of submission ○ Today
or select a day
● 21 June 2004

* denotes mandatory field

Select the service users to search for.
Select the service users to search for by clicking on the service user nummber. To select multiple service users, hold down the Ctrl key while you click on each service user. This is the service user/ bureau that made the submission.

Select to search for Live or Test submissions.

Select to search by File processing day...
Check the radio button, then select the start and end dates using the drop downs.

or

Select to search by Date of submission...
Check the “Date of submission” radio button, then select the appropriate radio button to either search over a period: today, last 2 days, last week, last 2 weeks, last month **OR** select a particular date.

Click *find*. If submissions match the search the *Live submissions* or *Test submissions* screen loads. If no submissions match, this screen reloads with an error.

To view submission information (continued)

3 Select the submission to view

The list of submissions contains basic information including the date and time it was submitted. It also tells you the status of the submission:

- Accepted – the submission has been accepted by BACS for processing (the submission could still fail main validation)
- Rejected – the submission has been rejected by BACS. This is normally due to structural validation errors. You can view the reasons for rejection
- Terminated – BACS stopped the submission coming through (see section 2.3, page 15 for information on when this could happen).

(This information will have already been included in the submission summary report that is sent to the software when a submission is made.)

To view more information about a submission, click on the serial number (rejected submissions do not have a serial number, but will have a hyperlink in the serial number column). The *Live submission summary* or *Test submission summary* screen loads.

4 View information on the submission

The screen shows a *Summary* section and a *File summary* section.

Summary – The *Summary* section shows:

- If the submission was rejected, you can click the *View reason for rejection* icon. A new browser opens displaying the *Rejection reason* screen. This shows errors that BACSTEL-IP returned to the submitting contact
- If this is a test submission, you can view the contents of the submission (the Standard 18 content) by clicking the *View entire submission* icon. A new browser opens showing the text of the submission.

File summary – The File summary block contains details of each payment file in the submission (if this was submitted by a service user, there will only be one file shown here):

- If there is a ⚠ icon, click this icon to view any warnings generated when the payment file was submitted. A new browser opens displaying these warnings
- If this is a test submission, you can view the contents of the submission (the Standard 18 content) by clicking the 🗎 icon. A new browser opens showing the text of the payment file.

Part VI

Managing your additional contacts

This part describes procedures for PSCs to add and maintain additional contacts. Only your sponsor can add and maintain PSCs.

General procedures for contacts to log on, get and change their own passwords and register their smartcards are in the *Contact's guide*, starting on page 69.

To add and maintain PSCs or to set up a contact associated with an HSM, please contact your sponsor.

To see a list of contacts linked to your service user, see section 8.5, page 36.

> *Note: To make any changes to an additional contact that has PKI security (or both security methods), or to add an additional contact with PKI security, you must be logged on to payment services with PKI. To add or maintain additional contacts with ASM you can be logged on with ASM or PKI. You also require the relevant privilege, see section 19, page 67 for a list of privileges.*

14 *Contact details* screen fields

These are the fields on the *Contact details* screen. Fields marked with an asterisk (*) are mandatory.

	Field	Contents
	Title	Free text up to 10 characters: Mr, Mrs, Dr etc. Once this field has been populated it cannot be changed.
*	First name/last name	Cannot be changed. 25 characters each.
*	Security method	Select from drop down: *digital certificate* (PKI), *contact ID and password* (ASM) or *both* (PKI and ASM). (If you add ASM security to a contact, you need to enter the *Registration information*, see below.)
	PKI status / ASM status	These are set by a combination of system and user action; see section 14.1, page 59.
*	Email address	Up to 50 characters. This is used to send notifications, welcome emails etc.
	Telephone numbers	The following information can be entered: • Office telephone area code (5 numerals) and number (10 numerals); extension (5 characters) • Out of office telephone code and number; mobile code and number; fax area code and number (area codes, 5 numerals; numbers, 10 numerals each) • Extra information (such as times to use the number) can be entered for the office and mobile number (40 characters each). It is recommended that at least one number is recorded for each contact.
	Exception / Out of hours contacts	These flags may be used by your sponsor to indicate a contact that is available to answer questions about submissions and/or is available to be contacted out of hours.
	HSM contact	This indicates if this contact is associated with a hardware security module (HSM). *Note: Only your sponsor can set up contacts with HSMs for you. For information on HSMs, see Security, page 16.*
*	Registration information	If the contact has ASM security this is where the security information and hint are recorded. (After they have been entered and confirmed, they are not displayed.) • The security information can be up to 40 characters (it is not case sensitive when used by the contact) • The security hint is up to 80 characters.
	Privileges	Privileges a contact has are displayed with ticks. Greyed out boxes means the privilege can only be assigned/removed by your sponsor. For a list of privileges, see section 19, page 67.

14.1 Statuses

A contact has a status for each security method. If a contact is having a problem logging on, you should check their status. These are described below.

Status	PKI/ASM	Details
Not set	PKI/ASM	The contact does not have this security method.
Active	PKI/ASM	The contact can use their security method for everything they are set up to do.
Pending	PKI/ASM	• For PKI, indicates the contact has not registered their smartcard (if they do not have their smartcard registration email, you can resend it to them, see section 16.2, page 63 • For ASM, indicates the contact has not got their contact ID and password (if they do not have their email to get their contact ID and password, you can reset their password, this sends a new email to them, see section 16.1, page 62).
Suspended	PKI/ASM	The contact cannot log on or perform any action using the security method they are suspended for. The suspension may be system generated, for example if a contact repeatedly enters the wrong password, or initiated by another contact. If a contact has a status of: • Suspended for all their security methods, they do not receive any notification emails • Pending before being suspended, their status displays as “Suspended – pending”. To “unsuspend” a contact’s security method, you reinstate it, see section 18, page 66.
Manual	PKI only	The contact’s DN has been manually entered by your sponsor (rather than the contact using their smartcard registration email to associate their DN with their contact profile). This is normally only done for HSM contacts. The PKI status automatically sets to “active” when the contact successfully logs on to payment services or using your BACSTEL-IP for the first time using their PKI.
Review	PKI only	The contact has captured their DN using the automated process and it is awaiting review by your sponsor. The contact cannot use their PKI security until they are active.

15 Adding additional contacts

These steps show you how to add a new contact to your service user or link an existing contact to your service user. After adding a contact with PKI, you must contact your sponsor, as PKI credentials have to be issued. If the contact is to make submissions, your sponsor has to assign the relevant privileges. (Only your sponsor can add PSCs.)

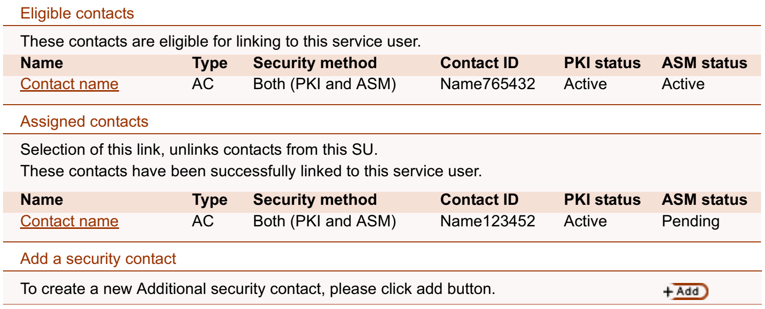
To add additional contacts

You must be logged on to payment services with ASM or PKI, and have the relevant privilege.

1 Select *Contact maintenance > Add new service user contact*

Select the *Contact maintenance* menu, then select *Add new service user contact*. Select the service user you need from the list. The *Service user contacts* screen loads.

2 Click add or select a contact



Eligible contacts

These contacts are eligible for linking to this service user.

Name	Type	Security method	Contact ID	PKI status	ASM status
Contact name	AC	Both (PKI and ASM)	Name765432	Active	Active

Assigned contacts

Selection of this link, unlinks contacts from this SU.
These contacts have been successfully linked to this service user.

Name	Type	Security method	Contact ID	PKI status	ASM status
Contact name	AC	Both (PKI and ASM)	Name123452	Active	Pending

Add a security contact

To create a new Additional security contact, please click add button.

These are contacts linked to other service users that are in the same organisation. You can link additional contacts to your service user

These are contacts linked to your service user

To link an eligible contact, click on their name. The *Summary* screen loads. Go to step 5.

To add a new contact, click *add*. The *Contact details* screen loads.

3 Enter the details of the contact

Enter the details of the contact and select a security method. For information on the fields on this screen, see section 14, page 58. Click *next*. The *Contact privileges* screen loads.

4 Select the privileges

Use the check boxes to select the privileges the contact needs. Click *submit*.

5 Check the summary and confirm using security credentials

Check the summary. If it is correct click *confirm*. The *Security check* screen loads:

- **If you are logged on with PKI,** your signing software opens. With your smartcard in the reader, use your PIN to sign the information
- **If you are logged on with ASM,** enter your password and click *OK*.

If successful, the Success screen loads. Emails are sent to the contact to allow them to register their smartcard and/or get their contact ID and password.

16 Maintaining additional contacts

Note: Only your sponsor can maintain PSCs.

To maintain additional contacts

You must be logged on to payment services with ASM or PKI, and have the relevant privilege.

1 Select the contact

Select the *Contact maintenance* menu, then *Maintain service user contact*. Search for the required contact by entering their first and/or last name or their contact ID. Click *find*. Select the contact from the returned list.

The *Contact details* screen loads.

2 Change the general details, security method and/or registration information as required

Make the necessary changes to the fields; see section 14, page 58 for details of the fields. (To change the security method, select the new security method from the drop down list. If you add ASM, you need to enter the security information and hint.)

After making the changes, click *next*. The *Contact privileges* screen loads.

3 Change the privileges if required and submit

In *Privileges*, select the privileges for the contact by selecting and unselecting the check boxes. For a full list of privileges, see section 19, page 67.

After making the necessary changes, click *submit*. The *Summary* screen loads.

4 Check the summary and confirm using security credentials

Check the summary. If it is correct click *confirm*. The *Security check* screen loads:

- **If you are logged on with PKI,** your signing software opens. With your smartcard in the reader, use your PIN to sign the information
- **If you are logged on with ASM,** enter your password and click *OK*.

If successful, the *Success* screen loads. If you:

- Removed PKI security, speak to your sponsor as the contact’s smartcard may have to be revoked (if it is not used for any other service)
- Added PKI, speak to your sponsor (if you have not already) to have a smartcard issued
- Added a security method to a contact, emails are sent to allow them to get their contact ID and password or register their smartcard.

16.1 Resetting passwords

You cannot reset a contact's password when they have an ASM status of suspended; you must first reinstate them. If a contact knows their password, but has repeatedly mistyped it and has become suspended, you can reinstate them and they can continue using their existing password.

When the password is reset, the contact receives an email with a link to allow them to access the new password. They will have to enter their security information. If they have forgotten this, you should change it; see section 16, page 61.

To reset a password

You must be logged on to payment services with ASM or PKI, and have the relevant privilege.

1 Select the contact

Select the *Contact maintenance* menu, then select *Maintain service user contact*. Search for the required contact by entering their first and/or last name or their contact ID. Click *find*. Select the contact from the returned list.

The *Contact details* screen loads.

2 Click *reissue password*

Click *reissue password*. The *Are you sure?* screen loads.

Click *OK* and the *summary* screen loads.

3 Check the summary and confirm using security credentials

Check the summary. If it is correct click *confirm*. The *Security check* screen loads:

- **If you are logged on with PKI,** your signing software opens. With your smartcard in the reader, use your PIN to sign the information
- **If you are logged on with ASM,** enter your password and click *OK*.

If successful, the *Success* screen loads. An email is sent to the contact to let them get their new password. The procedure for them to follow is in the *Contact's guide*, see section 33.2.2, page 114.

16.2 Managing PKI registration emails

The steps below support a contact when they are registering their PKI credentials. Two actions can be performed:

- **Resend the email** – if a contact has not registered their PKI credentials (and has a PKI status of pending), you can resend the email containing the unique web address for them to register their PKI credentials
- **Reregister the smartcard** – if a contact receives a new smartcard and is told by your sponsor that it has to be reregistered.

> *You must only use the reregister function if you have been told to do so by your sponsor. If you click reregister, the contact will no longer be able to use their existing smartcard on BACSTEL-IP. Normally, if a contact receives a new smartcard, their DN does not change, and therefore, the card does not have to be reregistered.*

To resend the PKI email or reregister PKI credentials

You must be logged on to payment services with PKI, and have the relevant privilege.

1 Select the contact

Select the *Contact maintenance* menu, then select *Maintain service user contact*. Search for the required contact by entering their first and/or last name or their contact ID. Click *find*. Select the contact from the returned list.

The *Contact details* screen loads.

2 Click *resend* or *reregister*

Depending on the contact's PKI status, one of the following buttons is displayed:

- **Resend**. Click *resend* to resend the contact's "Registering your smartcard" email
- **Reregister**. Click *reregister* to delete the contact's DN, send a new "Registering your smartcard" email to the contact and change their PKI status to pending.

The *Are you sure?* screen loads. Click *OK* and the summary screen loads.

3 Check the summary and confirm using security credentials

Check the summary. If it is correct click *confirm*. The *Security check* screen loads. With your smartcard in the reader, use your PIN to sign the information. If successful, the *Success* screen loads. An email is sent to the contact so they can register their smartcard. The procedure for them to follow is in the *Contact's guide*.

17 Deleting and unlinking additional contacts

Deleting a contact permanently removes them from BACSTEL-IP. If the contact is linked to more than one service user, this affects all service users the contact is linked to.

If a contact is linked to more than one service user, you can unlink them from a service user. This prevents them acting for the service user. If the contact is only linked to one service user, unlinking them deletes them from BACSTEL-IP. (The service users a contact is linked to are displayed on the *Contact details* screen in the bottom right of the *Contact details* section.)

When deleting a contact with PKI security, speak to your sponsor to arrange for the PKI credentials to be revoked (unless the person uses it for some other service offered by your sponsor).

Note: A deleted contact cannot be reinstated. To set a person up again, they need to be added as a new contact. If they use PKI, new PKI credentials must be issued.

17.1 Delete additional contacts

To delete a contact

You must be logged on to payment services with ASM or PKI, and have the relevant privilege.

1 Select the contact

Select the *Contact maintenance* menu, then select *Maintain service user contact*. Search for the required contact by entering their first and/or last name or their contact ID. Click *find*. Select the contact from the returned list.

The *Contact details* screen loads.

2 Click delete

Click *delete*. The *Are you sure?* screen loads. Click *OK* and the *Summary* screen loads.

3 Check the summary and confirm using security credentials

Check the summary. If it is correct click *confirm*. The *Security check* screen loads:

- **If you are logged on with PKI,** your signing software opens. With your smartcard in the reader, use your PIN to sign the information
- **If you are logged on with ASM,** enter your password and click *OK*.

If successful, the *Success* screen loads.

17.2 Unlink additional contacts

To unlink a contact

You must be logged on to payment services with ASM or PKI, and have the relevant privilege.

1 Select *Contact maintenance > Add new service user contacts*

Select the *Contact maintenance* menu, then select *Add new service user contact*. Select the service user you require.

The *Service user contacts* screen loads.

2 Select the contact to be unlinked from this service user

Under *Assigned contacts*, click on the name of the contact you want to unlink from this service user.

The screen reloads, the name will no longer be displayed under *Assigned contacts*. If the contact is still linked to another service user, their name will be displayed under *Eligible contacts*; otherwise this action will delete the contact.

Click *submit*. The summary screen loads.

3 Click unlink and confirm using your security credentials

Check the summary. If it is correct, click *confirm*. The *Security check* screen loads:

- **If you are logged on with PKI,** your signing software opens. With your smartcard in the reader, use your PIN to sign the information.
- **If you are logged on with ASM,** enter your password and click *OK*.

If successful, the *Success* screen loads.

18 Suspending and reinstating additional contacts

You can suspend (and subsequently reinstate) contacts for one or both of their security methods. You cannot suspend a contact's PKI status if it is set to "review". Suspending a contact prevents them using that security method to access BACSTEL-IP. When a contact is suspended, their status for the security method is displayed as "suspended" (or "suspended – pending" if they had a status of pending before being suspended). When a contact is reinstated, their status for that security method returns to what it was before being suspended.

If a contact is suspended for all their security methods, they do not receive any email notifications they are set up for.

Contacts can also be automatically suspended by the system. For example, if a contact repeatedly enters an incorrect password their ASM status is set to suspended.

To suspend or reinstate a contact

You must be logged on to payment services with ASM or PKI, and have the relevant privilege.

1 Select the contact

Select the *Contact maintenance* menu, then select *Maintain service user contact*. Search for the required contact by entering their first and/or last name or their contact ID. Click *find*. Select the contact from the returned list.

The *Contact details* screen loads.

2 Click *suspend* or *reinstate*

Click *suspend* or *reinstate*. The *Suspend contact* or *Reinstate contact* screen loads.

Using the drop down list, select the security methods you want to suspend/reinstate the contact for. Click *OK*.

The *Are you sure?* screen loads. Click *OK* and the *Summary* screen loads.

3 Check the summary and confirm using security credentials

Check the summary. If it is correct click *confirm*. The *Security check* screen loads:

- **If you are logged on with PKI,** your signing software opens. With your smartcard in the reader, use your PIN to sign the information
- **If you are logged on with ASM,** enter your password and click *OK*.

If successful, the *Success* screen loads.

19 Privileges

This section details privileges that can be assigned to service user contacts. There are some privileges that only your sponsor can assign to contacts; these are marked in the tables.

All contacts have the ability to log on to payment services, log on using BACSTEL-IP software (if they have PKI), view their own details, maintain their email address and telephone numbers and change their password (if they have one).

The tables in the following sections list the privilege name (that is displayed on screen), what the privilege allows the contact to do, the security methods and the contact types the privilege is available to (some privileges are only available to contacts with PKI and some are only available to PSCs). There are no privileges that are only available to additional contacts; there are no privileges that are only available with ASM security. Only privileges available to a contact are displayed on screen.

The privileges on screen are displayed in two groups: generic and three-day licence.

To change an additional contacts privileges, see section 16, page 61.

19.1 Generic privileges

Privilege name	Allows the contact to...	Security	Contact
Add and maintain contacts (ASM)	• Add, maintain and delete additional contacts that have ASM security • View service user information.	PKI/ASM	PSC
Add and maintain contacts (PKI)	• Add, maintain and delete additional contacts that have PKI and/or ASM security • View service user information.	PKI	PSC
Maintain own service user reference data (ASM)	• Maintain service user information (excluding setting the file signature flag).	PKI/ASM	PSC
Maintain own service user reference data (PKI)	• Maintain service user information (including setting the file signature flag).	PKI	PSC
Maintain service user and contact ASM	• Maintain service user information (excluding setting the file signature flag) • Add, maintain and delete additional contacts that have ASM security.	PKI/ASM	PSC
Maintain service user and contacts (PKI)	• Maintain service user information (including setting the file signature flag) • Add, maintain and delete additional contacts that have PKI and/or ASM security.	PKI	PSC
View own service user information	• View service user information.	PKI/ASM	PSC/AC

19.2 Three-day licence privileges

Privilege name	Allows the contact to...	Security	Contact
Report access privileges			
Access ARUDD and ARUCS advices*	• Access ARUDD and ARUCS advices.	PKI/ASM	PSC/AC
Access live processing reports*	• Access live processing reports.	PKI/ASM	PSC/AC
Access messaging reports*	• Access messaging reports.	PKI/ASM	PSC/AC
Access processing reports and advices*	• Access live processing reports • Access test processing reports • Access ARUDD and ARUCS advices.	PKI/ASM	PSC/AC
Access test processing reports*	• Access test processing reports.	PKI/ASM	PSC/AC
Submission and signing privileges			
Enquire on live submissions	• View information on live submissions	PKI	PSC/AC
Enquire on test submissions	• View information on test submissions • View the contents of test submissions.	PKI	PSC/AC
Sign live and test payment files	• Sign live and test payment files.	PKI	PSC/AC
Sign live and test payment submissions	• Sign live and test submissions.	PKI	PSC/AC
Submit and enquire on live and test submissions†	• Submit live and test submissions • Sign live and test payment files • Sign live and test submissions • View information on live submissions • View information on test submissions • View the contents of test submissions • Access live processing reports • Access test processing reports.	PKI	PSC/AC
Submit and enquire on test submissions†	• Submit test submissions • View information on test submissions • View the contents of test submissions • Access test processing reports.	PKI	PSC/AC
Submit live submissions†	• Submit live submissions.	PKI	PSC/AC

* These privileges allow a contact to access the report type over payment services (using PKI or ASM) and over BACSTEL-IP using their software (they must have PKI to do this).

† These privileges can only be assigned to a contact by your sponsor.

BACS payment services

Contact’s guide

BACS

About your *Contact's guide*

This part of your guide provides general information about using the payment services website, including information about the security used to access payment services and BACSTEL-IP (using your software).

It describes how you register your smartcard, get your contact ID and password and then log on. It also provides help if you are having any problems with your security.

Part VII Contacts

20 What is a contact?

A contact is an individual who has been registered to use payment services or facilities.

As a registered contact you will have a unique contact ID. Against your contact ID the following must be set up:

- Security method(s)
- Contact type
- Privilege groups
- Communication information.

The following sections provide more information about each of these.

Security methods

In order to access the payment services and facilities, all contacts must have one or more security methods assigned to them.

There are two security methods that can be used to access the payment services and facilities: PKI credentials (PKI), including a digital certificate, and contact ID and password (alternative security method – ASM). For more information, see Part X and Part XI.

As a contact you can be assigned PKI, ASM or both. Each security method you have assigned to you will have a status, for example “active”, “suspended”. Depending on the status of the security method, you will be able to use that security method to log on to the payment services web channel and perform actions you have been assigned the privileges to do. For more information on the payment services web channel see Part VIII, starting on page 75.

Contact types

There are two different types of contact:

- Primary security contacts (PSCs)
- Additional contacts (ACs).

A primary security contact (PSC) can normally carry out more functions than an additional contact, and there are some functions only a PSC can carry out. All contacts registered to access payment services and facilities must be set up as either a PSC or an additional contact. The decision as to whether you are a PSC or an additional contact will depend on the role you have when using payment services. The functions a PSC or an additional contact can perform will depend on the privileges they are given.

Privilege groups

All contacts must be assigned one or more privileges groups. Privilege groups contain one or more privileges which will allow you, as a contact, to carry out specific activities and functions with payment services. If you have a specific privilege group assigned to you, you will be able to carry out the functions allowed by the privileges in that group.

Privilege groups are assigned to you when you are registered as a contact for payment services, but these can be amended at any time. The privilege groups available for assigning to you depend on:

- Contact type (PSC or additional contact)
- Security method (PKI or ASM).

More privileges are available to PSCs and to contacts who have PKI credentials. There are no privilege groups that are exclusively available to additional contacts with ASM. In other words, all privilege groups that can be assigned to an additional contact with ASM could be assigned to any contact type. The privilege groups a contact is assigned will depend on the role they will have when using the payment services.

Communication information

Communication details are held for each contact registered to use the payment services, namely:

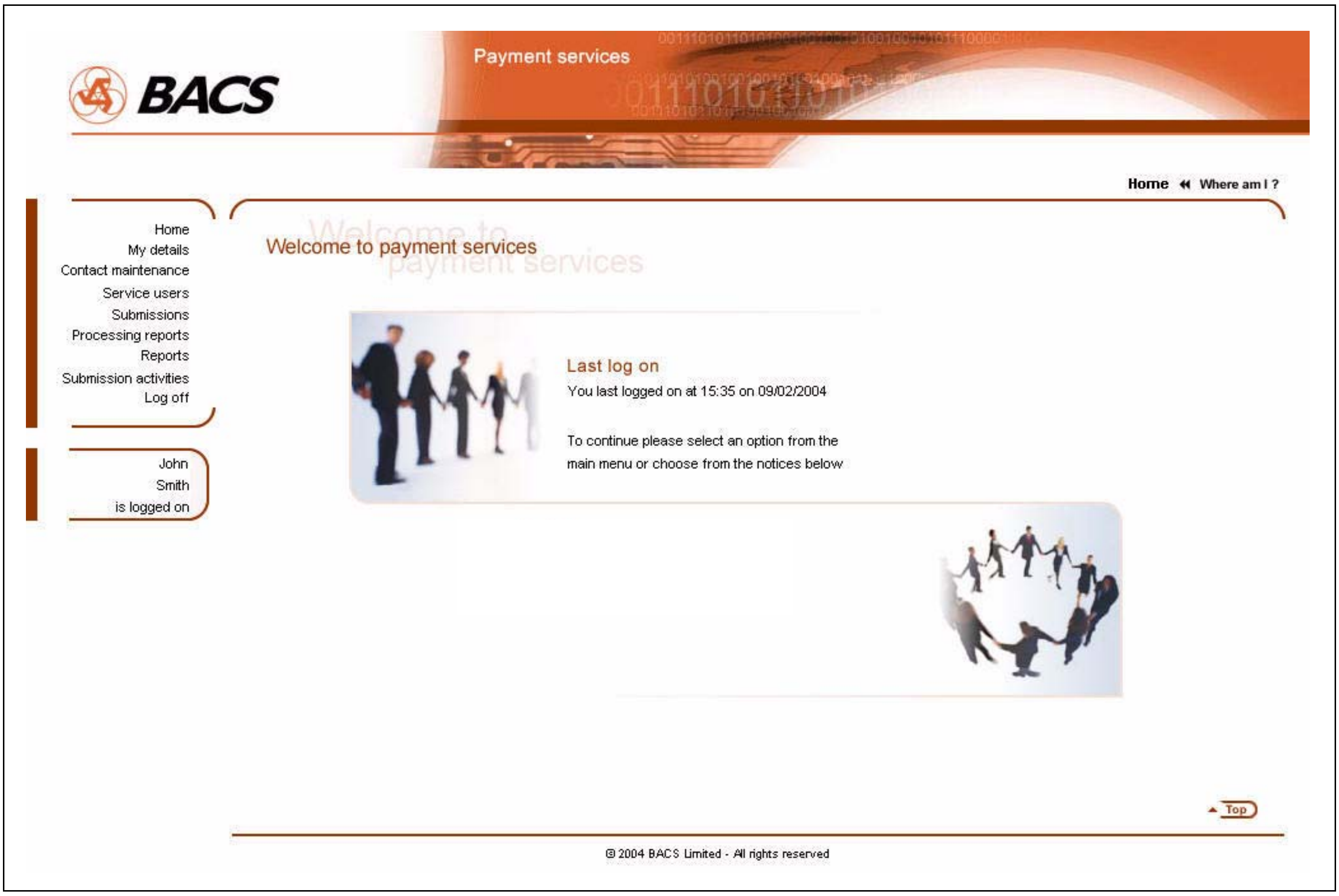
- Email address – mandatory
- Office telephone number, extension number and associated information – optional
- Out of hours telephone number – optional
- Mobile telephone number and associated information – optional
- Fax number – optional.

Part VIII

Payment services web channel

21 What is the payment services web channel?

As a registered contact for payment services and facilities, you can use your security method(s) to log on to the payment services web channel. The web channel is your way of accessing the payment services and facilities you have been set up to use and carry out the actions you have been given the privileges to do. The following diagram shows an example of the payment services web channel homepage. The exact features of your homepage will depend on what type of contact you are and what you can use the web channel for.



John Smith is logged on

Welcome to payment services

Last log on

You last logged on at 15:35 on 09/02/2004

To continue please select an option from the main menu or choose from the notices below

© 2004 BACS Limited - All rights reserved

Figure 7: An example of the payment services web channel homepage

Connections

To connect to the payment services web channel you will require the following:

- An internet browser
- A connection method (normally internet, but can be an extranet connection)
- A security method.

For information on software requirements, including internet browsers, see section 23, page 79. For more information on connection methods see section 24, page 80.

Security

You can log on to the web channel using PKI or ASM. If you have both PKI and ASM you can log on using either, however, if you log on with ASM, you may not be able to carry out all the functions you have been given the privileges to do.

For information on the privilege groups available for allocation to you and the security methods and contact types they can be assigned to see the guide(s) you have received regarding the services you have been set up to use.

Functionality

The payment services web channel can be used to access various features of the payment services and facilities you have been set up to use.

In addition to the features and facilities you have been set up to use, all contacts can use the payment services web channel to view and amend their own communication details

For more information on how to perform these actions on the web channel see Part XII.

Notifications

When many actions are carried out on the web channel, email notifications are generated and sent to relevant contacts. For example, if any of your contact details are changed by another contact, you will receive an email notification telling you that your details have been changed.

To make full use of the payment services and facilities you have been registered to use there may be additional requirements. If this is the case, the guide(s) you receive detailing the services and features will provide information on these additional requirements.

22 Availability

The web channel is available during the payment services window. This window normally opens at 07:00 hours on a Monday and closes at 23:00 hours on a Friday. English bank/public holidays also affect the opening times. The following table shows how the window opens and closes:

If the window is...	it will...
...open	...close at 23:00 hours the night before a nonprocessing day (a bank/public holiday, a Saturday or a Sunday).
...closed	...open at 07:00 hours on the first processing day after a nonprocessing day.

When the payment services window is open you can log on to the web channel. Once you are logged on, you can perform the functions you are set up to do over the web channel. For details of nonprocessing days see the processing calendar available from:

http://www.bacs.co.uk/resources/calendar.php

23 Software requirements

There are certain hardware and software requirements you must fulfil to access the web channel. The following sections detail the operating system and web browser requirements for connecting the BACS payment services web channel.

23.1 Web browsers

It is recommended that you use the latest version available of your chosen web browser.For information about browsers suitable for accessing the web channel using PKI contact your supplier of signing software. If you are using Internet Explorer you should ensure that your browser checks for newer versions of stored pages automatically. This is the default for your browser, but to check this setting and amend it if necessary carry out the following steps.

To set Internet Explorer page checking

You must have Internet Explorer installed.

1 Open Internet Explorer.

Open Internet Explorer on the computer you will use to access the web channel.

2 Access your internet options.

From Internet Explorer's *Tools* menu select *Internet Options...*

An *Internet Options* window will open. On the *General* tab, in the *Temporary Internet files* section, click the *Settings* button.

3 Amend your settings.

A *Settings* window will open. Ensure that the stored pages setting is set to *Automatic*. If not, click in the radio button, next to the word *Automatic*. Click *OK*, then click *OK on the Internet Options* screen.

23.2 Operating systems

In addition to a suitable browser, you must be running a suitable operating system on the computer you use to access the web channel. The following operating systems have been tested for connecting to the payment services web channel:

- Windows NT4 with service pack 5+
- Windows 98 SE
- Windows ME
- Windows 2000
- Windows XP.

24 Connection methods

Access to the payment services web channel will normally be via the internet. However, the web channel can also be accessed via the extranet. The following sections provide information for connecting via these two methods.

24.1 Internet

The normal method for connecting to the payment services web channel is via the internet. To access the payment services web channel over the internet, you should be connected to the internet and then go to the payment services web address (URL). When you receive your welcome email from BACS payment services, this will provide you with the web address (URL) that you should use.

24.2 Extranet

If required, you can connect to the payment services web channel via the extranet. Voca offers a fixed extranet, DSL connection, Broadband Direct and a dial-up extranet.

Fixed extranet, DSL Connect and Broadband Direct

If you would like more information about connecting to Voca over a fixed extranet, DSL Connect or Broadband Direct connection visit:

www.voca.co.uk/connectivity

Dial-up extranet

Although connecting to the payment services web channel is normally done over the internet, it can also be done via the dial-up extranet facility.

When connecting to the dial-up extranet one of two numbers[1] is dialled:

- 0870 241 6764
- 0870 163 6300.

An extranet ID and password are also required for connecting to the web channel via the dial-up extranet. An extranet ID and password can be used to connect to payment services by up to 10 different contacts at the same time. That is, up to 10 computers can be connected to the dial-up extranet at the same time using the same extranet ID and password.

[1] *These numbers are subject to change. Your system should allow for these numbers to be altered when necessary.*

If you have the use of more than one extranet ID and password you can use any of them to connect. However, the maximum number of concurrent connections with the same extranet ID and password is still 10. If 10 contacts are connected to the dial-up extranet using the same extranet ID and password, you will not be able to connect. There is no check made between the person logging on and the extranet ID that has been used to establish the dial-up connection.

If you require more information about how to go about utilising the dial-up extranet contact the service desk or your sponsor, if you have one.

25 Payment services web channel – Features and tools

The following sections provide an overview of how you can navigate around the web channel and the features and tools you will use when carrying out activities on the web channel.

Note: Fields shown on a page on the payment services web channel that are marked with an asterisk (*) are compulsory. You must complete these fields to successfully carry out the activity.

25.1 Navigating the web channel

Navigating the payment services web channel is much the same as other websites, with buttons and hyperlinks providing access to different areas and screens.

Most screens have on-screen navigation buttons that should be used for going “back” and for cancelling actions. You must not use the browser’s own buttons when logged on to the web channel as some pages may not load correctly. For example, do not use the browser’s back, forward, refresh or home buttons.

25.2 Online help

There is help available on the web channel. To access the help information available, click the *Help* button on the top right hand corner of the page. The help information should be used in conjunction with any other documentation you have received.

Clicking the *Help* button will open a new window, in which the help information will be displayed. Along with any help information, there will be a link to the help main menu. From the help main menu you can browse to help information for other pages.

25.3 Areas of the web channel screen

All web channel screens have some areas that are the same or similar. The following figure shows a typical web channel screen, highlighting the key areas that are the same or similar across all screens. The names of these ares, and details of their functions, are provided in the table that follows.

.

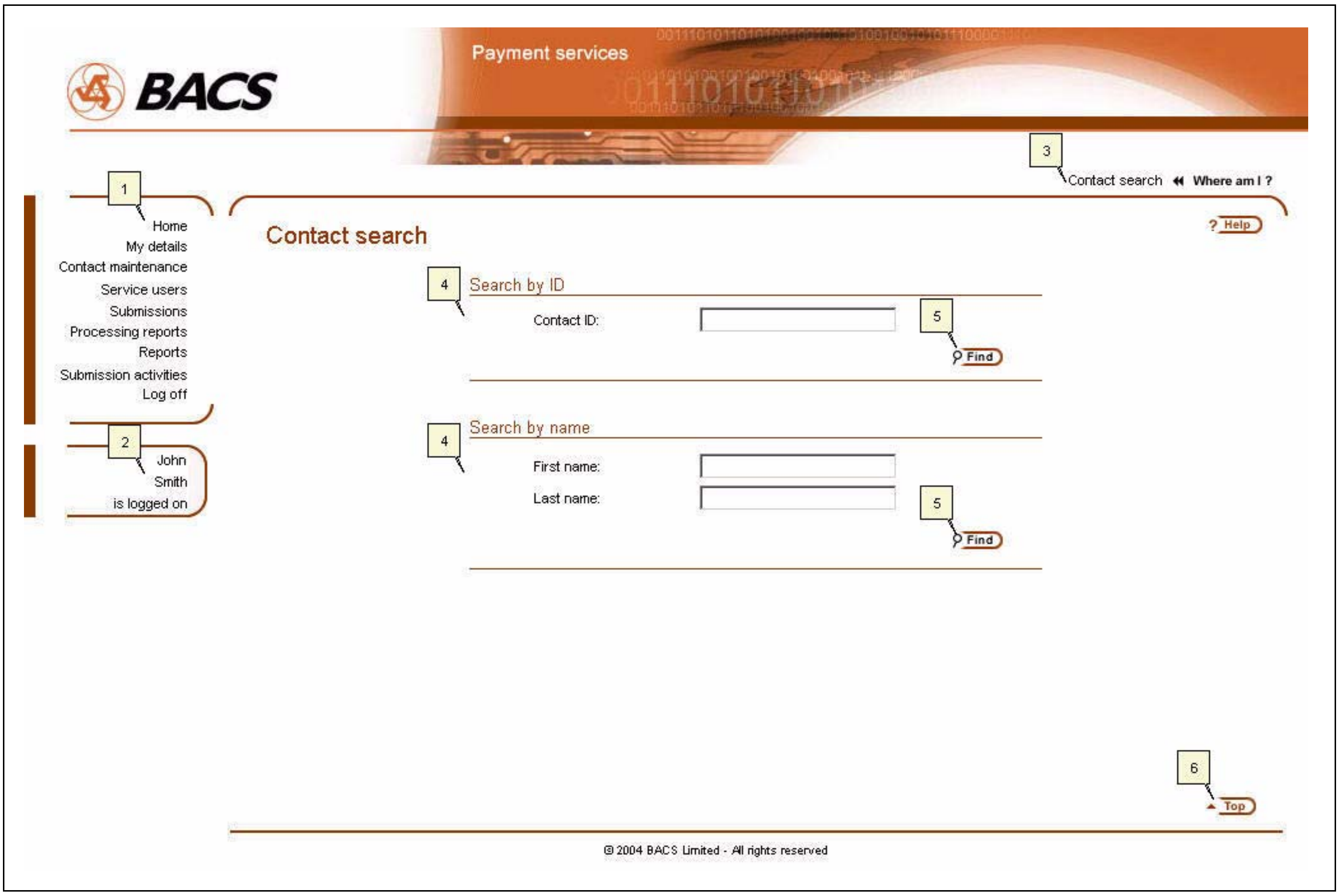
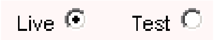
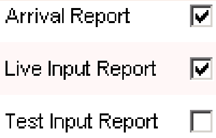
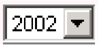
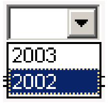
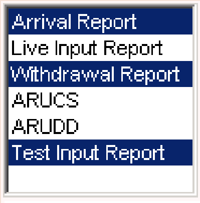


Figure 8: The areas of a web channel screen

Area	Name	Function	When seen
1	Menu	Selecting a menu option takes you to that area of the web channel.	Same on all pages.
2	Contact identification	Shows the first name and surname of the contact who is logged on.	Same on all pages.
3	“Where am I?” bar	Shows where in the web channel you are at that moment.	Differs on each page to reflect where you are.
4	Section block	The area of the screen where you can action something or view/confirm information. Some screens have several section blocks.	Different blocks appear on different pages.
5	Action buttons	There are a variety of different buttons on the web channel. The icon and the wording illustrates what each button does. To carry out the function a button provides, click the cursor on the button.	Different buttons appear on different pages.
6	Top button	Takes you to the top of the screen you are on. If you are at the bottom of a long screen you can click this button to take you back to the top.	Same on all pages.

25.4 Selection methods

The web channel uses standard selection methods for choosing options, dates etc. The following table details the different selection methods you will come across on the web channel and how to use them.

Type and example	What you can select	How to use the selection method
Radio button  Live ● Test ○	One option only.	To select, click in the circle next to the option you want (in the example "Live" is selected). To select a different option, click in the circle next to the new option you want. This will deselect the original option.
Check box  Arrival Report ☑ Live Input Report ☑ Test Input Report □	One or more options.	The selected option(s) is shown as a box with a tick. In the example, "Arrival Report" and "Live Input Report" are selected. To select options, click in the box next to the options required. Ticks will appear in all boxes you click in. To deselect an option click in the box again. This will remove the tick.
Drop down list  2002  2003 2002	One option only.	The selected option is shown in the box next to the drop down list. In the example "2002" has been selected. To select an option click on the arrow on the right side of the box. A list of options appears. Move the cursor until the option you want is highlighted and click it. The option you selected will be displayed in the box. To select a different option, repeat the above steps.
Pick list  Arrival Report Live Input Report Withdrawal Report ARUCS ARUDD Test Input Report	One or more options.	Selected options are highlighted. In the example, "Arrival Report", "Withdrawal Report" and "Test Input Report" are selected. To select, click on the option. This will highlight it. To select a different option, click on it. This will highlight the new option and deselect all other options. To select more than one option, hold down the "*Ctrl*" key on your keyboard which clicking each of the options you want. Clicking on a highlighted option will deselect it (hold down the "*Ctrl*" key to keep the other options selected). To select a group of options, hold down the "*Shift*" key on your keyboard and click on the first and the last options from the group that you want. This will highlight the two you clicked and all options in between. Alternatively, to select several options together, click on the first option you want and, while holding down the mouse button, drag the cursor down the list until all the options you want are highlighted.
Action button 	Used to perform a function.	To carry out an action, click on the button. Many buttons have additional information about the functioning of the button which can be viewed by hovering the cursor over the button. If additional information is available, a box of text will appear.

25.5 Find functionality

A number of activities on the web channel require a “find” to be done to look for the required information. Search types that are used on the web channel include:

- Name searches (name, first name or surname)
- ID searches.

These search types use different searching methods. The different search methods are “full text” and “part text” searches.

25.5.1 Full text search

A “full text” search means that you enter all the characters that you are searching for. For example, if you are looking for a contact whose contact ID is *smith123456* you would type each character of the contact ID into the find box.

25.5.2 Part text search

A “part text” search means that you can enter just some of the characters you are searching for. For example, if you are looking for someone whose surname is *Smith* you could type *Smi* or just *S* into the find box. The only constraint is that you must start your part text with the first character – you could not search by typing *mith* to find *Smith*.

Only some search types can use part text. The following table illustrates which search types can be done using part text searching, and provides additional notes on each search type.

Search type	Full text searching	Part text searching	Notes
Name search	✓	✓	Not case sensitive.
First name search	✓	✓	You can search for the first name, surname or both. Not case sensitive.
Surname search	✓	✓	
Organisation ID	✓	✗	Case sensitive.
Contact ID	✓	✓	Not case sensitive.

25.6 Request messages, commands and error messages

On the web channel, red text will sometimes appear above section blocks. This text may be:

- A request message; or
- A command; or
- An error message.

The text will provide you with an instruction on how to complete the screen you are on, or explain why your last request was not successful, or advise you of the action you have completed.

Part IX

Security overview

26 Overview

Access to payment services is controlled with high levels of security. To access payment services as a registered contact, you must identify yourself and pass security checks. There are two security methods that can be used to access the payment services web channel:

- Public key infrastructure (PKI)
- Contact ID and password (alternative security method – ASM).

As a contact, you must have at least one of these security methods. Fewer privileges can be given to contacts who only have a contact ID and password. If you have both security methods (PKI and ASM) you may not be able carry out all the functions you have been set up to carry out if you access the payment services using your contact ID and password.

When you carry out actions on the payment services web channel you will have to authorise the actions. For details on how to confirm actions see section 28.4, page 102. You must confirm actions using the same security method that you used to log on to the web channel.

Note: When using PKI to log on to the web channel, this guide assumes these PKI credentials are on a smartcard. It is not expected that contacts will log on to the web channel using an HSM. For information about HSMs please contact your solution supplier.

Part X provides information about PKI security and some fundamental PKI procedures. Part XI provides information about ASM security and some fundamental ASM procedures. The information in these parts includes how the security methods work, what the different methods are used for and what you will receive if you are set up for that method.

Part X

Security information & procedures – PKI

27 Security information: PKI

27.1 What are PKI credentials?

PKI uses digital keys and digital certificates to provide security for electronic communications and data transfers. This security provides authenticity and integrity.

A contact’s PKI credentials are made up of their digital keys and their digital certificate. These PKI credentials are issued (directly or indirectly) by a certification authority.

The following introduces some of the common terms you will hear in relation to PKI security:

Term	Definition
Certification authority (CA)	A trusted third party that issues and manages digital keys and certificates. During secure communications, the CA associated with a contact's digital certificate is contacted to confirm if the name given on the digital certificate is the one that is associated with the public key on the certificate.
Digital keys	A contact has two sets of digital keys: a private key and a public key. A contact's private key is only known to the contact. A contact's public key can be known by anyone.
Digital certificate	A "document" that contains, among other things, a copy of the contact's public key, details of the contact's name, the contact's assigned "distinguished name" and the expiry details of the certificate. The certificate is signed by the certification authority's own private key as proof that the contact's digital certificate is genuine.
Distinguished name (DN)	A unique piece of information allocated to a contact, partly based on their name, which is held on the contact's digital certificate. This information is recorded by BACS for all registered PKI credentials.

In this guide, "PKI" is used to refer to all aspects of a contact's PKI credentials required to carry out the security processes described in Part XI.

27.2 Storage of PKI credentials

A contact's PKI credentials are normally issued and held on a smartcard. The following diagram provides an overview of a smartcard and how a contact's PKI credentials are held on it.

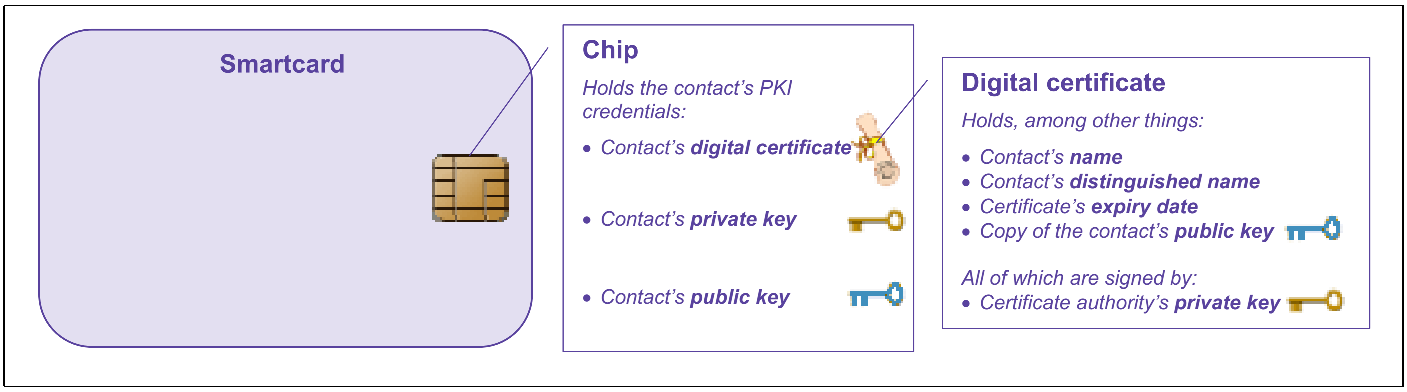

Smartcard
Chip
Holds the contact's PKI credentials:
• Contact's digital certificate
• Contact's private key
• Contact's public key
Digital certificate
Holds, among other things:
• Contact's name
• Contact's distinguished name
• Certificate's expiry date
• Copy of the contact's public key
All of which are signed by:
• Certificate authority's private key

Figure 9: A stylised diagram of a smartcard and PKI credentials

PKI credentials can also be held on a hardware security module (HSM). An HSM is used by companies who require a high volume of automated digital signing and verification.

27.3 Using PKI with payment services

27.3.1 What PKI is used for

You can use your PKI credentials to do the following:

- Log on to the payment services web channel
- Confirm actions you have carried out on the payment services web channel.

You will also be able to use your credentials to perform specific activities you have been given the privilege group(s) to do for the payment services and functions you can use.

If you have PKI credentials, you are obliged to use them when invited to do so by the payment services web channel.

27.3.2 What you need

If you have a PKI credentials stored on a smartcard, you will need the following to use your credentials to create digital signatures and authenticate yourself when using payment services:

- Smartcard reader
- Signing and decryption software
- PIN (personal identification number)[1].

Your PIN is used to control the security of your smartcard, and your PKI credentials stored on it. Your PIN is specific to your smartcard and is issued when your smartcard is issued to you. The PIN (which may contain alpha characters as well as numbers) must be entered each time you use your smartcard to digitally sign data.

Similar security measures exist for the operation of HSMs. However, once activated, the signing and decryption are generally fully automated and do not require further human intervention until the HSM is shut down.

[1] *Some signing software refers to PINs as a “passphrase”.*

27.3.3 How PKI security works with payment services

If you have PKI credentials on a smartcard, you can use these for logging on to payment services and authorising actions on the web channel. The following describes how PKI security works with payment services.

Logging on

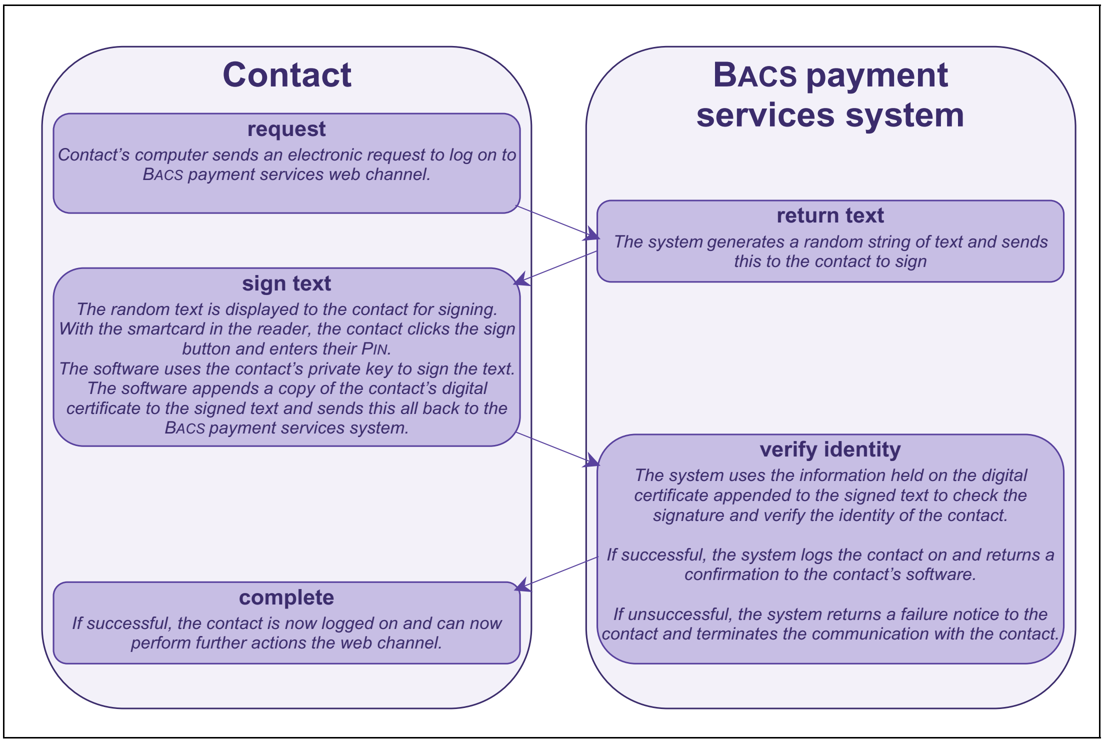
To authenticate you as a contact, when you log on to payment services with your PKI credentials, the BACS payment services system will send you a string of random text. Your signing software will load on your computer and will display this string of random text.

To authenticate yourself, you will have to “digitally sign” the random string of text. To do this, you must insert your smartcard into your smartcard reader attached to the computer and enter your PIN into the software. Your software will then “digitally sign” the string of text by processing the data using your private key. This produces a digital signature. The digital signature is then sent back to the BACS payment services system along with a copy of your digital certificate.

If the BACS payment services system is unable to validate your digital signature, the system will reject the data and terminate the action. This may be because:

- The data may have been altered since being digitally signed, either intentionally or accidentally; or
- The private key used to create the digital signature does not match the public key contained within the copy of your digital certificate that was appended to the data; or
- The BACS payment services system was not able to verify with the certification authority that your digital certificate is still valid (ie that it has not been revoked or is unknown) and that there is a valid link to the root certification authority (the highest level of trust within the PKI scheme).

The following diagram gives an overview of the processes involved in logging on to payment services with PKI security. A similar process is carried out when confirming an action on the payment services web channel, except the text to be digitally signed details the nature of the action being confirmed.



Contact

request

Contact's computer sends an electronic request to log on to BACS payment services web channel.

sign text

The random text is displayed to the contact for signing. With the smartcard in the reader, the contact clicks the sign button and enters their PIN.
The software uses the contact's private key to sign the text. The software appends a copy of the contact's digital certificate to the signed text and sends this all back to the BACS payment services system.

complete

If successful, the contact is now logged on and can now perform further actions the web channel.

BACS payment services system

return text

The system generates a random string of text and sends this to the contact to sign

verify identity

The system uses the information held on the digital certificate appended to the signed text to check the signature and verify the identity of the contact.

If successful, the system logs the contact on and returns a confirmation to the contact's software.

If unsuccessful, the system returns a failure notice to the contact and terminates the communication with the contact.

Figure 10: An overview of PKI security processes for logging on to BACS payment services

Confirming an action

To confirm an action on the payment services web channel using your PKI credentials, you will have to carry out a similar process as that described for logging on. However, instead of the BACS payment services system sending you a string of random text, the system will send you data that relates to the information you are confirming you want processed. It is this data that you will digitally sign to confirm the action.

28 Security procedures: PKI

28.1 Overview

PKI credentials stored on a smartcard can be used to access payment services. Before you can use your smartcard it must be activated. The following sections detail how to activate your smartcard for use with payment services, and then how to use your smartcard to log on to the payment services web channel and perform activities and functions on the web channel.

What you will need

Before you can start using PKI security to access payment services, you will need to wait until you have the following:

- Your smartcard
- A smartcard reader
- Signing and decryption software
- Your PIN.

How you receive your PIN with vary depending on your card supplier. Your card supplier may be your sponsor, if you have a sponsor. Your PIN may arrive before your smartcard (or vice versa). You must ensure that you keep both securely and separately until you are ready to get started.

28.2 Smartcard activation

28.2.1 Overview

Before you can use your PKI credentials on your smartcard to carry out any function, there are certain activation activities that need to be carried out. The following list details the activities that must be carried out before you can use your smartcard for the first time:

- Smartcard initialisation
- DN registration
- System checks
- Welcome email and first log on.

The following flow diagram provides an overview of these activation activities.

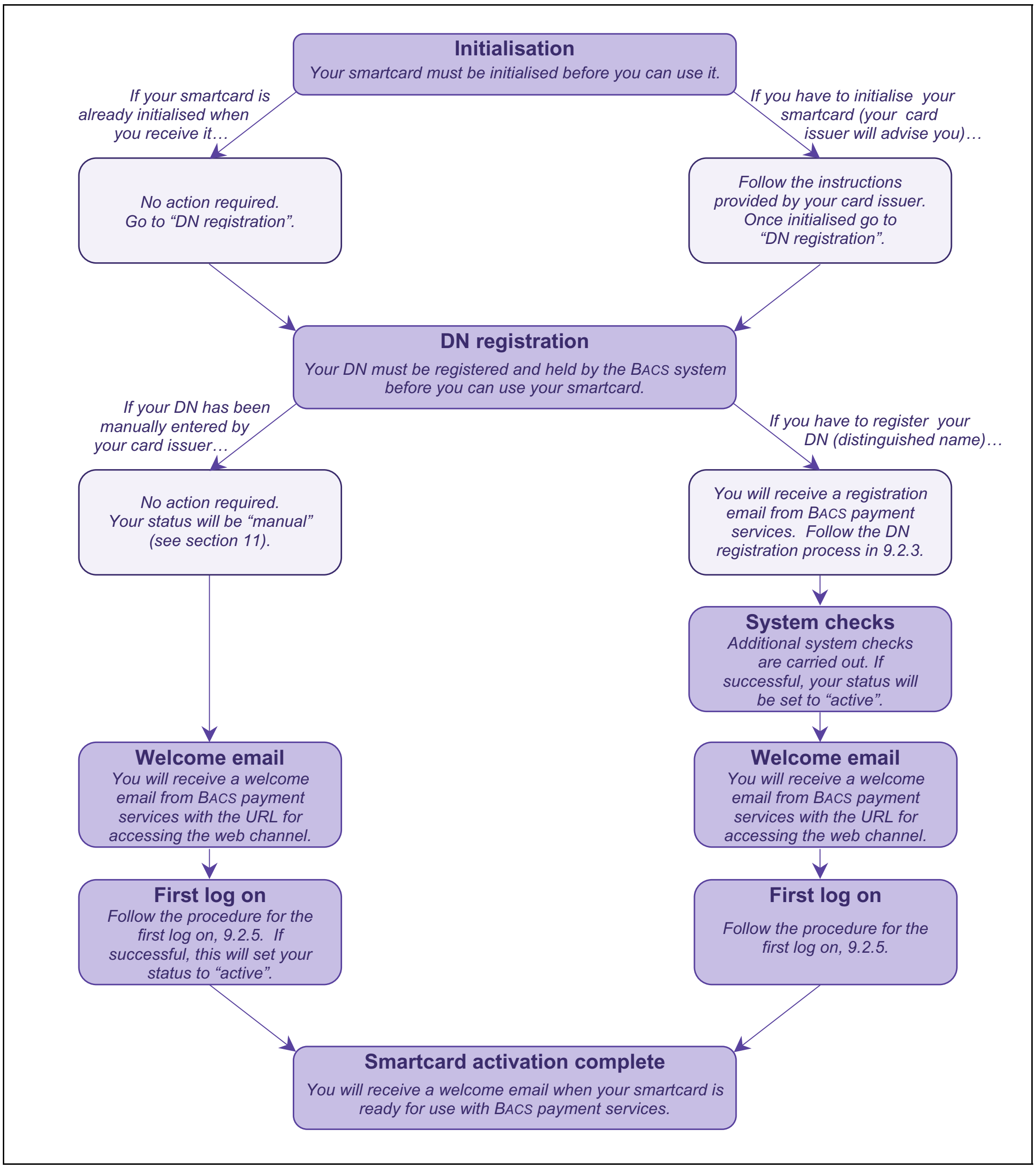

Initialisation
Your smartcard must be initialised before you can use it.
If your smartcard is already initialised when you receive it…
If you have to initialise your smartcard (your card issuer will advise you)…
No action required. Go to "DN registration".
Follow the instructions provided by your card issuer. Once initialised go to "DN registration".
DN registration
Your DN must be registered and held by the BACS system before you can use your smartcard.
If your DN has been manually entered by your card issuer…
If you have to register your DN (distinguished name)…
No action required. Your status will be "manual" (see section 11).
You will receive a registration email from BACS payment services. Follow the DN registration process in 9.2.3.
System checks
Additional system checks are carried out. If successful, your status will be set to "active".
Welcome email
You will receive a welcome email from BACS payment services with the URL for accessing the web channel.
Welcome email
You will receive a welcome email from BACS payment services with the URL for accessing the web channel.
First log on
Follow the procedure for the first log on, 9.2.5. If successful, this will set your status to "active".
First log on
Follow the procedure for the first log on, 9.2.5.
Smartcard activation complete
You will receive a welcome email when your smartcard is ready for use with BACS payment services.

Figure 11: Overview of the smartcard activation process

The above diagram is an overview, and exact processes may differ depending on the smartcard issuer. For specific details of the actions you must carry out, please refer to any instructions you have received from your card issuer.

You can find more information about each of these activities in the following sections. If you are issued with a replacement smartcard you must check with your card supplier which of these activities you will need to carry out.

28.2.2 Smartcard initialisation

A smartcard must be initialised before it can be used. Your card supplier may provide you with a smartcard that has already been initialised. If not, you may have to carry out an initialisation procedure. Your card supplier will advise you as to whether you need to initialise your smartcard, and if you do will provide you with details of the initialisation process.

28.2.3 DN registration

Before you can use your initialised smartcard, the DN or "distinguished name" on your digital certificate must be registered with and stored on the system.

Your DN can be registered with on the system, or by an automatic process. The following sections explain each of these.

Manual registration

Your card supplier may register your DN manually on the system. This means that you will not have to carry out the automated registration process described below. If your card supplier does register your DN manually, you will have a PKI status of "manual". For more information on statuses see section 30, page 104.

Your card supplier should inform you whether your DN has been registered manually, or whether you have to carry out the automated registration process. However, if you receive an email from BACS payment services with a subject of "BACS Payment Services – Registering your smartcard" you will have to carry out the automated registration process. If you do not receive this email, but do receive a "Welcome to BACS payment services" email your DN has been manually registered and you can go straight to section 28.2.5, page 99.

Note: All DNs for PKI credentials held on HSMs will be manually registered.

Automated registration process

You may need to carry out the automated registration process to register your DN on the system. Your card supplier should inform you whether you need to carry out this registration process. However, if you receive an email from BACS payment services with a subject of "BACS Payment Services – Registering your smartcard" you will have to carry out this automated registration process. If you do not receive this email, but do receive a "Welcome to BACS Payment Services" email your DN has been manually registered (see above) and you can go straight to section 28.2.5, page 99.

If you need to carry out the automated registration process, your "BACS Payment Services – Registering your smartcard" email will contain a unique URL (web address). These instructions should be used in conjunction with the following procedure.

Your registration email should be on, or easily transferred to, the computer that you will use to access the payment services web channel. If this cannot be done, you can find instructions in the following procedure on how to copy the URL from the email to the computer that will be used to access the web channel.

If you accidentally delete your registration email you can have it resent. To organise having it resent, contact a PSC who can maintain your details, your sponsor, if you have one, or the service desk.

Note: Do not attempt to carry out the following procedure if you do not have the following:

- *Your registration email with registration URL*
- *Your initialised smartcard*
- *Your PIN*
- *A smartcard reader and associated signing software on the computer that you will use to access the web channel.*

To register your DN

You must have your registration email, your initialised smartcard and your PIN.

1 Establish a connection to the internet (or extranet).

Connect to the internet, or the extranet if this will be used to access the web channel.

2 Go to your registration URL.

Open the email “BACS Payment Services – Registering your smartcard” and click on the URL (web address). Your web browser will open and the *Digital certificate registration* screen will load.

Alternatively, copy the registration URL from the email, open a web browser and paste the URL into the address bar. Press the *Enter/Return* key on your keyboard.

If your registration email is on a different computer, than that used to access the web channel, and it cannot easily be transferred, copy the URL from the email and paste it into a Microsoft Word, Notepad or other document and save it to a disk. Open this document on the computer that will be used to access the web channel. Copy the URL from the document and paste it into your web browsers address bar. Press the *Enter/Return* key on your keyboard.

To register your DN (continued)

3 Confirm your name.

The *Digital certificate registration* screen displays the contact name associated with the URL.

If this is your name, click *confirm*.

If this is not your name, check that you have used the correct email. If you are using the correct email and your name is incorrect, contact a PSC who can maintain your details. The PSC should check your details on the web channel.

4 Signing software opens. Insert your smartcard and sign the random text.

Your signing software will automatically open. Insert your smartcard into your reader.

A random string of text will be displayed in the signing software window. To authenticate yourself, you must digitally sign this string of text. To do this, click the *sign* or *sign and submit* button on your signing software. You will need to enter your PIN.

5 A screen loads stating that you have successfully registered your digital certificate.

If the registration process was successful, a screen loads informing you. You can now close your browser.

Note: Although your registration process may have been completed successfully, system checks need to be carried out. You must now wait until those checks are complete and you have received your welcome email before you use your smartcard for anything.

28.2.4 System checks

Once your DN is registered on the system, additional system checks are carried out. If your DN was manually registered you will still have a status of “manual” after successful completion of system checks. If you registered your DN through the automatic process, your status will become “active” if system checks are successful.

When the system checks have been successfully completed, you will receive a welcome email from BACS payment services.

28.2.5 Welcome email and first log on

When the system checks have been successfully completed, you will receive your “Welcome to BACS payment services” email. Your welcome email contains the web address you must use for accessing the web channel with your smartcard.

You can now carry out the procedure for logging on to the web channel for the first time. If your DN was manually registered (you have received your welcome email and have not had to carry out the automatic registration procedure) carrying out the first log on procedure successfully will change your status from “manual” to”active”.

First log on

You must carry out the following procedure, once your welcome email arrives, before you use your smartcard for anything else. The following procedure details how to log on for the first time, and how to create a shortcut to BACS payment services for ease of logging on in the future.

To log on for the first time with PKI

You must have your welcome email, your initialised/registered smartcard and your PIN.

1 Establish a connection to the internet (or Voca extranet).

Connect to the internet, or the Voca extranet if this will be used to access the web channel.

2 Go to your welcome URL.

Open the email “Welcome to BACS payment services” and click on the URL (web address). Your web browser will open and the *Log on* screen will load.

Alternatively, copy the welcome URL from the email, open a web browser and paste the URL into the address bar. Press the *Enter/Return* key on your keyboard.

If your email is on a different computer, than that used to access the web channel, and it cannot easily be transferred, you can write the URL down and type it into your web browser’s address bar. Press the *Enter/Return* key on your keyboard.

To log on for the first time with PKI (continued)

3 Create a shortcut to the web address.

When the *Log on* screen loads, and your signing software opens, click your mouse on the web browser window. This will ensure that it is the web browser window that is active, and not the signing software. The signing software will stay open in front of the web browser, but will be the inactive window.

Press *Ctrl* + *D*. This will create a shortcut to BACS payment services that can be accessed through the *Favourites* menu of Internet Explorer and the *Bookmarks* menu of Netscape Navigator.

4 Sign the random text.

Click your mouse on the signing software window to make it the active window. Your signing software will present you with a random string of text to sign that will authenticate you to the web channel. Sign the text by doing the following:

- Insert your smartcard into your reader (if it is not already inserted)
- Click the *sign* or *sign and submit* button on your signing software
- Enter your PIN.

5 BACS payment services web channel homepage loads.

If the authentication process was successful, the web channel homepage will load into your browser, and your name will appear in the contact identification area of the page (see section 25.3, page 82 for details of the screen areas).

You can now carry out activities on the web channel, and your smartcard is now ready to use for all the activities and functions you have been given the privileges to do.

28.3 Logging on

After you have completed the first log on procedure (*First log on*, page 99) you can use your smartcard to log on to the payment services web channel and perform the functions you have been given the privileges to do. The following section describes how to log on to the web channel using your PKI credentials which involves authenticating yourself to the web channel.

To log on to the web channel with PKI (after first log on)

You must have carried out the first log on procedure for PKI.

1 Establish a connection to the internet (or Voca extranet).

Connect to the internet, or the Voca extranet if this will be used to access the web channel.

2 Open your web browser.

If you already have a browser open, you should close it and open a new browser window.

3 Go to your BACS payment services web channel shortcut.

If your browser is Internet Explorer, click on the *Favourites* menu and choose BACS payment services from the drop down list.

If your browser is Netscape Navigator, click on the *Bookmarks* menu and choose BACS payment services from the drop down list.

The *Log on* screen will load.

4 Sign the random text.

Your signing software will present you with a random string of text to sign that will authenticate you to the web channel. Sign the text by doing the following:

- Insert your smartcard into your reader (if it is not already inserted)
- Click the *sign* or *sign and submit* button on your signing software
- Enter your PIN.

5 BACS payment services web channel homepage loads.

If the authentication process was successful, the web channel homepage will load into your browser, and your name will appear in the contact identification area of the page (see section 25.3, page 82 for details of the screen areas).

Note: If you log on to the web channel and you do not perform any activity on the web channel (the session is idle) for 10 minutes, the session will time out. You will have to reauthenticate yourself before you can perform any more activities on the web channel. To reauthenticate yourself, carry out the log on procedure from step 4 onwards.

28.4 Actioning changes

When you change or add/delete information on the web channel, you will be asked to confirm that you wish to make the change(s). You must confirm the changes using the security method you logged on to the web channel with. The following procedure details how to confirm changes using your PKI credentials. For information on how to confirm changes using your contact ID and password, see section 33.4, page 120.

To action changes using PKI credentials

You must have logged on using your PKI credentials and made changes on the web channel.

1 Review a summary of your changes and accept them.

A *Summary* screen is displayed detailing the changes you are making. If the summary is correct, click *confirm* to start the process of actioning the changes.

2 Authorise the changes by signing the text displayed.

A confirmation screen will be displayed where you authorise the changes by entering your security credentials. If you logged on to the web channel with your PKI credentials, and are therefore authorising the changes with your PKI credentials, your signing software will load, displaying text detailing the change(s) you are going to make. Enter your PIN to sign the text. You will “digitally sign” the text displayed, and hence sign the change(s) you are making.

If the changes were made successfully, a *Success* screen will load. In some circumstances, eg your browser crashing, you may not see the success screen. Should this occur, you should check whether the changes you input have been applied.

If at any point, before signing the text, you decide you do not want to make the change(s) click the *cancel* or *back* action buttons on the screen. Depending on the stage you are at you may be taken to:

- A screen asking “Are you sure” you want to cancel the activity
  - Click *yes* to lose any changes that have not been confirmed, or
  - Click *no* to go back to confirm the changes or to make further changes.
- A maintenance screen where you can
  - Make further changes, or
  - Click *cancel* to be taken to the cancel activity screen (see first bullet point).

Note: Following many changes actioned on the payment services web channel, email notifications are sent by BACS payment services to the PSCs associated with the contact making the changes. The email notifications detail what was changed, who made the change(s) etc.

29 Protecting your smartcard and PIN

As your PIN is not known to anyone other that yourself, if you forget your PIN you will need to contact your card supplier as your smartcard may need to be replaced.

Some smartcards will allow you to change your PIN, others will only allow you to change it the first time you use it, others will not allow you to change it at all. If you would like to change your PIN you should read the documentation that accompanied your signing software.

Note: Contact your card issuer immediately if you have any smartcard problems.

- *Do NOT write your PIN down.*
- *If you think your PIN has been compromised, contact your card supplier immediately. Do not use your smartcard until your card supplier has advised you of what action to take.*
- *If you lose your smartcard you must contact your card issuer immediately.*

30 PKI statuses

If you have been set up for PKI security, you will have a PKI security status. To use your smartcard, you will need to have a PKI status of “Active”. There are other possible statuses that you could have. The following table details the possible statuses that you may have for your PKI security, and what it means if you have that status.

Status	What it means
Not set	You have not been set up to have PKI credentials for accessing payment services.
Active	You can use your PKI credentials for everything you have been set up to do. If you are set up to use the BACS electronic funds transfer service, you must have a status of active before you can sign payment files or submissions.
PKI pending	You have not yet registered your DN. For details of how to register your DN see section 28.2.3, page 96.
Suspended	You cannot log on or perform any action using your PKI credentials. The status of “Suspended” may have been automatically generated by the BACS payment services system following an incident (eg you have logged on to BACS payment services but your digital certificate has been revoked). The status of “Suspended” may have been set by your card issuer, your sponsor (if you have one), Voca or a PSC who can amend your details, through the process of suspending a contact. If you also have a contact ID and password, providing your ASM status is “active”, you can continue to carry out everything you have been set up to do using your contact ID and password, providing it is not a PKI only activity. If you only have PKI security, or if you ASM status is also “Suspended”, you will no longer receive any notification emails.
Suspended - Pending	As for “Suspended”, you cannot log on or perform any action using your PKI credentials. You were in a state of “PKI pending” before you were suspended, and, if you are reinstated, your status will revert to “Pending”. If you also have a contact ID and password, providing your ASM status is “active”, you can continue to carry out everything you have been set up to do using your contact ID and password, providing it is not a PKI only activity. If you only have PKI security, or if your ASM status is also “Suspended”, you will no longer receive any notification emails.
Manual	Your DN has been manually registered on the system. Your status will automatically change to “Active” the first time you log on the BACS payment services using your PKI credentials, providing the DN on your smartcard matches the DN held by on the system.
Review	You have registered your DN and your sponsor (if you have one) is going to review your DN. Providing the DN registration process was successful, your sponsor will set your status to “Active”.

31 Issues with your PKI security

This section details the possible issues you may experience with your PKI security, and actions you can take to overcome them.

Issue and description	Action
DN registration issues	
Email deleted/cannot be accessed You have deleted/cannot access your email with your unique URL for DN registration, and have not registered your DN.	You will need to arrange to have the email resent. To do this, in the first instance you should inform a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor if you have one or the service desk.
Email on a different computer You cannot access your email, with your unique URL for DN registration, on the computer that you are going to use to access the web channel.	It is recommended that the email is available on the same computer as the one you will use to access the web channel (which must have a smartcard reader and related software installed). If this is not possible: • Copy the URL from the email and paste it into a document (eg Microsoft Word, Notepad). • Save the document containing the URL to a disk. • Open the document on the computer with the web channel access. • Copy the URL from the document and paste it into your web browser. • Press *Enter/Return* key on your keyboard to go to the link.
URL does not work You web browser returns an error saying the page cannot be found when you try use your unique URL for registering your DN.	You should ensure that you are properly connected to the internet (or Voca extranet, if this is used). If the URL has been copied, or cut and pasted, ensure the correct URL is in the address bar or your browser. If this URL still does not work, contact the Voca service desk.
Name displayed is not correct After going to your unique URL, the name displayed on the first page is not yours.	You should check you are using the correct email (and correct URL). If you are, in the first instance contact a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor if you have one or the service desk. They must ensure your name and email address are correct on the web channel. If they are, they should contact the service desk.
Technical error During DN registration, the web channel returns a “technical error”.	You should reattempt the action using the same URL.
“Try again later” message During DN registration, the web channel returns a “try again later” message.	You should reattempt the action using the same URL.
Failure message You attempt to register your DN. The web channel returns a “Digital certificate – registration failure” message.	You should reattempt the action using the same URL. If it still does not work, you should contact a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor if you have one or the service desk.

Issue and description	Action
First log on issues	
Failure message You attempt to log on for the first time and the web channel returns a failure message.	You should reattempt the action. If it still does not work, you should contact a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor, if you have one, or the service desk.
No welcome email Your welcome email has not arrived.	Contact a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor, if you have one, or the service desk.
Smartcard and/or PIN issues	
PIN forgotten You have forgotten your PIN.	You must inform your card issuer immediately.
Incorrect PIN entered You have entered an incorrect PIN. Your signing software has returned an error saying the PIN was incorrectly entered.	You must enter your PIN again.
Incorrect PIN entered repeatedly You have entered the wrong PIN consecutively and the card has become locked. Your signing software returned a message saying a PIN had been entered incorrectly, but there may not have been a message saying the card is locked.	You must inform your card issuer immediately. You may have to be issued with a replacement card and/or PIN. You may have to be reinstated over the web channel (your PKI status may be “Suspended” or “Suspended – pending”) before you can use your new smartcard/PIN. *Note: The number of times the PIN needs to be entered incorrectly before the card is locked depends on the card issuer.*
Card lost You have lost your smartcard.	You must inform your card issuer immediately. You will then be suspended for PKI until your new smartcard is available.
Card cannot be read Your smartcard cannot be read. This may be due to damage.	Try to identify any equipment problem by trying the card on another computer, if one is available. If the card still does not work, you must inform your card issuer immediately. You will be issued with a new smartcard.
Other smartcard issues	
New smartcard with new DN You have been issued with a new smartcard with a new DN.	You may have to register your new DN. If you do, you will receive an email containing a new unique URL to carry out the registration process. If you do not receive your email, contact a PSC who can maintain your details. If a PSC cannot maintain your details contact your sponsor, if you have one, or the service desk. If you need to initialise the smartcard, your card issuer will give you the details.
New smartcard You have been issued a new smartcard.	You will not have to carry out the DN registration process if your DN has not changed. If you were suspended for PKI, your will have to be reinstated for PKI. If you need to initialise the smartcard, your card issuer will give you the details.
Digital certificate expired You attempt to log on and the web channel returns a failure message.	You should contact your card issuer. You will be issued with a new smartcard. Your card issuer will advise you whether you have to initialise your smartcard, and whether your new smartcard has a new DN.

Issue and description	Action
Suspended for PKI security You have been suspended automatically for PKI. This can occur for a number of reasons, eg digital certificate invalid, digital certificate expired etc.	You will need to be reinstated for PKI by a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor, if you have one, or the service desk. Any other issues must be resolved before you can log on again with your smartcard.
All other issues	You should contact your card issuer, a PSC who can maintain your details, your sponsor (if you have one) or the BACS service desk.

Part XI

Security information & procedures – ASM

32 Security information: ASM

32.1 What is ASM security?

The “alternative security method” (ASM) uses a contact ID and password to provide security for electronic communications and data transfers. The contact ID and password are issued by payment services, and the password is then changed by the contact to one of their choice.

In this guide, “ASM” is used to refer to a contact using their contact ID and password to carry out the security processes described in this guide.

32.2 Using a contact ID and password with payment services

32.2.1 What ASM is used for

You can use your contact ID and password to do the following:

- Log on to the payment services web channel
- Authorise actions you have carried out on the BACS payment services web channel.

You will also be able to use your contact ID and password to perform specific activities you have been given the privilege(s) to do for the payment services and functions you can use.

32.2.2 What you need

If you have a been registered for ASM, you will need the following to use payment services:

- Contact ID
- Password.

To obtain your contact ID and password, you will need the following:

- A piece of security information, eg *Smith*
- A hint to your security information, eg *Mother’s maiden name*
- Unique URL (web address) in an email from BACS payment services.

32.2.3 How ASM security works with payment services

If you have a contact ID and password, you can use these for logging on to BACS payment services and confirming actions on the web channel.

Logging on

To authenticate you as a contact, when you log on to the payment services web channel with your contact ID and password, you must enter your contact ID and password in the required fields. If the password you have entered is correct for that contact ID you will be logged on to the web channel.

Confirming an action

To confirm an action on the payment services web channel using your contact ID and password, you will have to carry out the same process as that described for logging on.

33 Security procedures: ASM

33.1 Overview

Before you can use ASM to log on to the payment services web channel you will need to retrieve your contact ID and password. This is done using the web channel. The following sections detail how to retrieve your contact ID and password, and then how to log on the payment services web channel and perform activities and functions on the web channel.

33.2 Contact ID and password activation activities

33.2.1 Overview

Before you can use ASM to access payment services you must carry out the following activities:

- Retrieve your contact ID and temporary password, using your unique web address
- Log on for the first time
- Change your password.

The following diagram provides an overview of these activities.

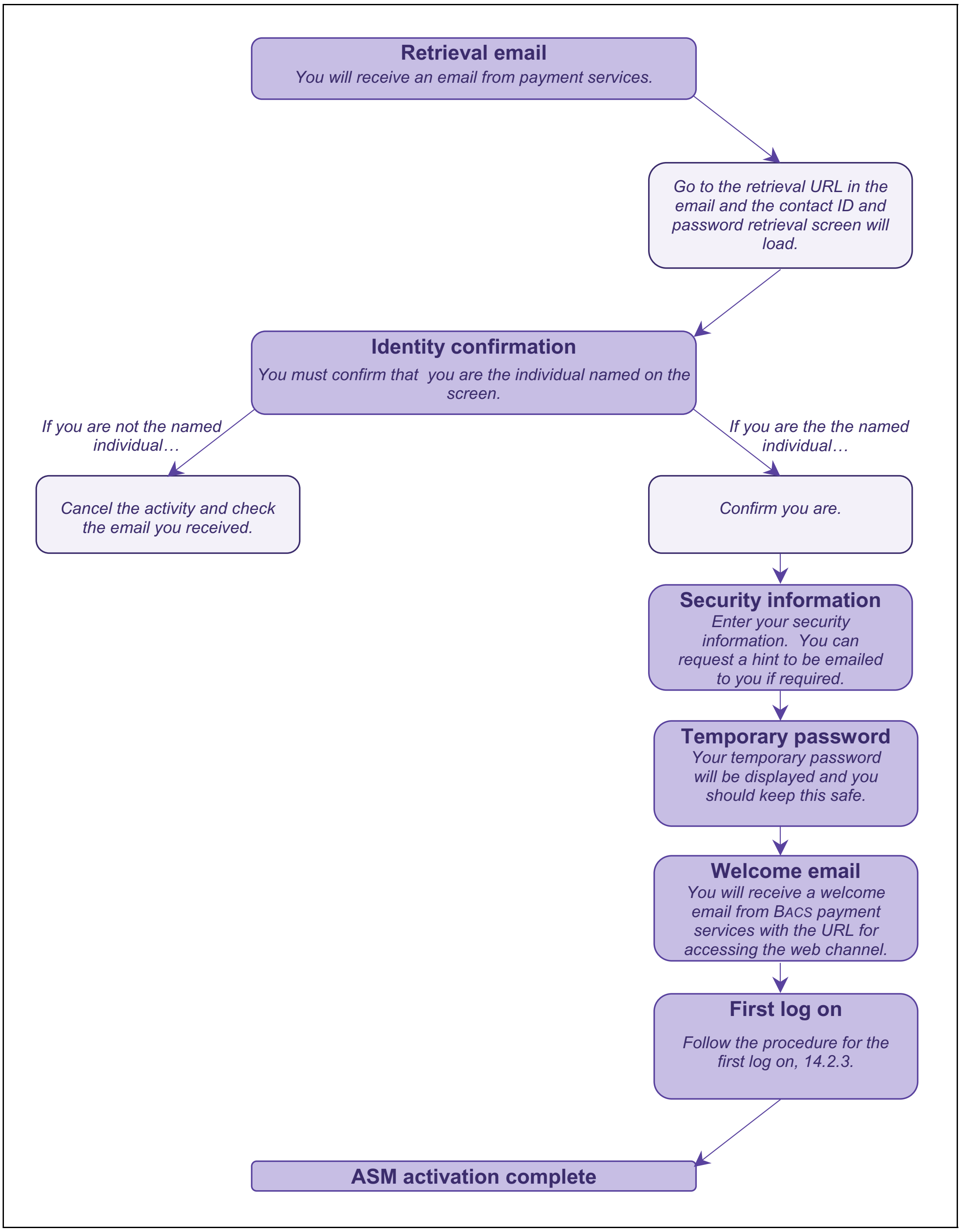

Retrieval email
You will receive an email from payment services.
Go to the retrieval URL in the email and the contact ID and password retrieval screen will load.
Identity confirmation
You must confirm that you are the individual named on the screen.
If you are not the named individual…
If you are the the named individual…
Cancel the activity and check the email you received.
Confirm you are.
Security information
Enter your security information. You can request a hint to be emailed to you if required.
Temporary password
Your temporary password will be displayed and you should keep this safe.
Welcome email
You will receive a welcome email from BACS payment services with the URL for accessing the web channel.
First log on
Follow the procedure for the first log on, 14.2.3.
ASM activation complete

Figure 12: Overview of the ASM retrieval process

You can find more information about each of these activities in the following sections.

When you are set up with ASM security, to access payment services, a piece of security information and a hint for that information is registered for you. This could be for example:

Security information	*Smith*
Hint	*Mother's maiden name*

When you retrieve your contact ID and temporary password you will need to enter your security information. This information is not case sensitive. If you cannot remember your security information, you can request to have the hint emailed to you before you try to retrieve your ASM details again.

Once you have carried out the above activities you can use your contact ID and password to access BACS payment services. If you wish to change your password you can do this over the web channel. For details on how to change your password see section 33.5.1, page 121.

If your password is ever reset by someone, which is different from you changing your password, you will receive a new retrieval email. You will have to use this to retrieve your new password, but your contact ID will remain the same. If your password is reset you will have to carry out all of the activities as described in the following sections.

33.2.2 Contact ID and password retrieval

To use ASM to access payment services, you must first retrieve your contact ID and a temporary password. To retrieve your contact ID and password you will receive an email from BACS payment services with a subject of “BACS Payment Services – Your contact ID and password”. This email will contain a unique URL (web address).

Your ASM retrieval email should be on, or easily transferred to, the computer that you will use to access the BACS payment services web channel. If this cannot be done, you can find instructions in the following procedure on how to copy the URL from the email to the computer that will be used to access the web channel.

If you accidentally delete your ASM retrieval email you can have it resent. To organise having it resent, contact a PSC who can maintain your details or, if you have a relationship with a sponsoring bank, contact your sponsor or the service desk.

Note: Do not attempt to carry out the following procedure if you do not have your email containing your contact ID and password retrieval URL and your security information. If you have forgotten your security information, you can elect to have the hint emailed to you. How to do this is explained in the following email. If you still cannot remember your security information even with the hint, a PSC who can maintain your details, your sponsor, if you have one, or the service desk change your security information and hint for you.

To retrieve your contact ID and password

You must have your ASM retrieval email and you must know your security information.

1 Establish a connection to the internet (or Voca extranet).

Connect to the internet, or the Voca extranet if this will be used to access the web channel.

2 Go to your security retrieval URL.

Open the email “BACS Payment Services – Your contact ID and password” and click on the URL (web address). Your web browser will open and the *Contact ID and password registration* screen will load.

Alternatively, copy the retrieval URL from the email, open a web browser and paste the URL into the address bar. Press the *Enter/Return* key on your keyboard.

If your retrieval email is on a different computer, than that used to access the web channel, and it cannot easily be transferred, copy the URL from the email and paste it into a Microsoft Word, Notepad or other document and save it to a disk. Open this document on the computer that will be used to access the web channel. Copy the URL from the document and paste it into your web browsers address bar. Press the *Enter/Return* key on your keyboard.

To retrieve your contact ID and password (continued)

3 Confirm your name.

The *Contact ID and password registration* screen displays the contact name associated with the URL in the *Confirmation* block.

If this is your name, click *confirm*.

If this is not your name, check that you have used the correct email. If you are using the correct email and your name is incorrect, contact a PSC who can maintain your details. The PSC should check your details on the web channel.

4 Enter your security information.

A new screen will load. You must enter your security information. Your security information is *not* case sensitive and when you type it, it will appear on screen as asterisks (*). Click *confirm*.

If you cannot remember your security information, you can have the hint emailed to you. To do this, click the *sent hint* button. You will then receive an email from BACS payment services which includes the hint to your security information. Once this email arrives you should restart this procedure.

5 Make a note of your contact ID and temporary password.

If you entered your security information correctly, the screen will reload with your contact ID and temporary password displayed. You must make a note of these carefully. Your temporary password is case sensitive but will only contain capital letters and numbers.

KEEP YOUR CONTACT ID AND TEMPORARY PASWORD SECURE until your welcome email arrives.

Your ASM status will now be set to “Active” but you must now wait until you receive your welcome email before logging on to the payment services web channel for the first time. Keep your contact ID and temporary password securely.

33.2.3 Welcome email and first log on

When you have retrieved your contact ID and temporary password you will receive a “Welcome to BACS Payment Services” email. Your welcome email contains the web address you should use for accessing the web channel with your ASM details.

First log on

You can now carry out the procedure for logging on to the web channel for the first time. The following procedure details how to log on for the first time, how to change your temporary password, and how to create a shortcut to payment services for ease of logging on.

To log on for the first time with ASM

You must have your welcome email, your contact ID and password.

1 Establish a connection to the internet (or extranet).

Connect to the internet, or the extranet if this will be used to access the web channel.

2 Go to your welcome URL.

Open the email “Welcome to BACS Payment Services” and click on the URL (web address). Your web browser will open and the *Log on* screen will load. Alternatively, copy the welcome URL from the email, open a web browser and paste the URL into the address bar. Press the *Enter/Return* key on your keyboard.

If your email is on a different computer, than that used to access the web channel, and it cannot easily be transferred, you can write the URL down and type it into your web browser’s address bar. Press the *Enter/Return* key on your keyboard.

3 Create a shortcut to the web address.

The *Log on* screen loads. If you do not have a smartcard reader installed on your computer, press *Ctrl + D*. This will create a shortcut to BACS payment services that can be accessed through the *Favourites* menu of Internet Explorer and the *Bookmarks* menu of Netscape Navigator. If you have a smartcard reader installed on your computer your signing software will open. Click your mouse on the web browser window. This will ensure that it is the web browser window that is active, and not the signing software. The signing software will stay open in front of the web browser, but will be the inactive window. press *Ctrl + D*. This will create a shortcut to BACS payment services that can be accessed through the *Favourites* menu of Internet Explorer and the *Bookmarks* menu of Netscape Navigator. Now close the signing software window.

Note: If there is a shortcut to BACS payment services on your computer already you can use that rather than the URL in your email, and you do not have to create a new shortcut.

To log on for the first time with ASM (continued)

4 Enter your contact ID and password.

Type your contact ID and temporary password into the correct fields. Note that your contact ID and password are case sensitive.

Click the *log on* button. This process will authenticate you to the web channel.

5 *Password change* screen loads. Change your password.

Type your temporary password into the correct field. Then enter your new password into the correct fields. You will have to enter your new password twice. This is also case sensitive. For details of the required format for passwords see section 33.5.2, page 122.

Click *done* to change your password.

6 BACS payment services web channel homepage loads.

If the password change process was successful, the web channel homepage will load into your browser, and your name will appear in the contact identification area of the page (see section 25.3, page 82 for details of the screen areas).

You can now use your contact ID and password to carry out activities and functions on the web channel.

33.3 Logging on

After you have completed the first log on procedure you can use your contact ID and password to log on to the payment services web channel and perform the functions that you have been given the privileges to do that can be done with ASM security. The following sections describe how to use your contact ID and password to log on to the web channel, which involves authenticating yourself to the web channel.

To log on to the web channel with ASM (after first log on)

You must have carried out the first log on procedure for ASM.

1 Establish a connection to the internet (or extranet).

Connect to the internet, or the extranet if this will be used to access the web channel.

2 Open your web browser.

If you already have a browser open, you should close it and open a new browser window.

3 Go to your BACS payment services web channel shortcut.

If your browser is Internet Explorer, click on the *Favourites* menu and choose BACS payment services from the drop down list.

If your browser is Netscape Navigator, click on the *Bookmarks* menu and choose BACS payment services from the drop down list.

The *Log on* screen will load.

4 Enter your contact ID and password.

When the *Log on* screen loads, if you have a smartcard reader installed on your computer your smartcard signing software will load. If you wish to continue logging on with your contact ID and password, close the signing software.

To log on with your contact ID and password, enter your contact ID and password (both are case sensitive) into the correct fields and click the *log on* button. This process will authenticate you to the web channel.

5 BACS payment services web channel homepage loads.

If the authentication process was successful, the web channel homepage will load into your browser, and your name will appear in the contact identification area of the page (see section 25.3, page 82 for details of the screen areas).

If the authentication process was unsuccessful an error message will appear on the screen and you should try again.

Note: If you log on to the web channel and you do not perform any activity on the web channel (the session is idle) for 10 minutes, the session will time out. You will have to reauthenticate yourself before you can perform any more activities on the web channel. To reauthenticate yourself, carry out the log on procedure from step 4 onwards.

If you repeatedly enter your password incorrectly, you will become suspended for ASM. You should contact a PSC who can maintain your details or your sponsor, if you have one. If you know your password, they will be able to reinstate you for ASM and you can continue using your password. If you have forgotten your password it will they will need to reset it for you as well as reinstating you. If your password is reset you will have to carry out the procedure detailed in section 33.2.2, page 114.

If you password becomes compromised you must immediately contact Bacs or your sponsor, if you have one.

33.4 Actioning changes

When you change or add/delete information on the web channel, you will be asked to confirm that you wish to make the change(s). You must confirm the changes using the security method you logged on to the web channel with. The following procedure details how to confirm changes using your contact ID and password. For more information on how to confirm changes with PKI credentials, see section 28.4, page 102.

To action changes using ASM

You must have logged on using your ASM details and made changes on the web channel.

1 Review a summary of your changes and accept them.

A summary screen is displayed detailing the changes you are making. If the summary is correct, click *confirm* to start the process of actioning the changes.

2 Authorise the changes by signing the text displayed.

A confirmation screen will be displayed where you authorise the changes by entering your security credentials. If you logged on to the web channel with your contact ID and password, and are therefore authorising the changes with your ASM details, you must enter your password. Enter your ASM details in the correct fields.

If the changes were made successfully, a *Success* screen will load. In some circumstances, eg your browser crashing, you may not see the success screen. Should this occur, you should check whether the changes you input have been applied.

If at any point, before entering your password, you decide that you do not want to make the change(s) click the *cancel* or *back* action buttons on the screen. Depending on the stage you are at you make be taken to:

- A screen asking “Are you sure” you want to cancel the activity
  - Click *yes* to lose any changes that have not been confirmed, or
  - Click *no* to go back to confirm the changes or make further changes
- A maintenance screen where you can
  - Make further changes, or
  - Click *cancel* to be taken to the cancel activity screen (see first bullet point).

Note: Following many changes actioned on the payment services web channel, email notifications are sent by BACS payment services to the PSCs associated with the contact making the changes. The email notifications detail what was changed, who made the change(s) etc.

33.5 Your password

33.5.1 Changing your password

The following section describes how to change your password for logging on to the web channel with ASM security. When choosing a new password, choose something that others will not be able to guess. For example, do not use your name and date of birth. If you forget your password you should contact a PSC who can maintain your details, your sponsor (if you have one) or the service desk to have your password reset.

Note: If your password has been compromised you must immediately contact the service desk or your sponsor, if you have one. See section 33.5.3, page 122 for more information.

To change your password

You must have logged in to the web channel and you can view the menu.

1 Select *My details* from the menu.

Click on the *My details* menu option to load the *My details* screen.

2 Click the *change password* button.

The *My details* screen loads. Click the *change password* button.

3 *Change password* screen loads. Enter your current and new passwords.

In the *Change password* block there are three fields (existing password, new password and re-enter new password).

- Enter you current password into the first field
- Enter what you would like to be your new password in the second field (for details of the format for passwords see section 33.5.2, page 122)
- Enter you new password again into the third field
- Click *OK* to change your password.
- If successful, go to step 4. If unsuccessful, carry out this step again to change your password.

If you decide that you do not want to change your password click *back* instead of clicking *OK*.

To change your password (continued)

4 *My details* screen loads and your password has been changed. Click *confirm* or *cancel* or select a new menu option.

If required you can make other changes to your details (see section 36.2, page 128). Otherwise click *cancel* or select a new menu option.

Note: After changing your password, if you click confirm from the My details screen, the actioning sequence runs. If you logged on with your contact ID and password you must use your NEW password to authorise the changes.

33.5.2 Password specifications and guidelines

The password for ASM is case sensitive. When selecting a new password it should meet the following specifications:

Specification	Example
Password must be at least seven characters in length	incorrect *december31* correct *dec3mber1*
Password must contain at least two numeric characters	
The numeric characters must not all be at the start and/or end of the password	
Password must not contain two consecutive identical characters	incorrect *logg1ng7* correct *log3ing1*
Password must not be the same as any of the past 12 passwords used	
Password must not be the same as your contact ID	

33.5.3 Protecting your password

You must ensure that your password is something you will remember, and you must always keep it safe. Do not write your password down.

If you think that your password has been compromised, you must immediately contact the service desk or your sponsor, if you have one. You must not then log in until the service desk or your sponsor has advised you that you can. Your password will need to be reset before you can log on again and this will involve you retrieving a new password (see section 33.2.2, page 114).

33.5.4 Changing you security information and hint

If you need to change your security information and hint, you must contact a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor if you have one, or the service desk.

34 Issues with your ASM security

This section details the possible issues that you may experience with your ASM security, and actions you can take to overcome them.

Issue and description	Action
Contact ID and password retrieval issues	
Email deleted/cannot be accessed You have deleted/cannot access your email with your unique URL for ASM retrieval, and have not retrieved your ASM details.	You will need to arrange having the email resent. To do this, you should inform a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor, if you have one, or the service desk.
Email on a different computer You cannot access your email, with your unique URL for ASM retrieval, on the computer that you are going to use to access the web channel.	If is recommended that the email is available on the same computer as the one you will use to access the web channel (which must have a smartcard reader and related software installed). If this is not possible: • Copy the URL from the email and paste it into a document (eg Microsoft Word, Notepad). • Save the document containing the URL to a disk. • Open the document on the computer with the web channel access. • Copy the URL from the document and paste it into your web browser. • Press *Enter/Return* key on your keyboard to go to the link. Alternatively, you can write the URL down, and type it into your web browser address bar, and press *Enter.*
URL does not work You web browser returns an error saying the page cannot be found when you try use your unique URL to retrieve your ASM details.	You should ensure that you are properly connected to the internet (or BACS extranet, if this is used). If the URL has been copied, or cut and pasted, ensure the correct URL is in the address bar or your browser. If this URL still does not work, contact the service desk.
Name displayed is not correct After going to your unique URL, the name displayed on the first page is not yours.	You should check you are using the correct email (and correct URL). If you are, contact a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor, if you have one, or the service desk. They should ensure your name and email address are correct on the web channel. If they are, they should contact the service desk.
Technical error During ASM retrieval, the web channel returns a “technical error”.	You should reattempt the action using the same URL.
“Try again later” message During ASM retrieval, the web channel returns a “try again later” message.	You should reattempt the action using the same URL.
Security information is not accepted You attempt to retrieve your ASM details. Your security information is not accepted by the web channel and an error is returned.	You should reattempt the action using the same URL. Ensure that you are using the correct case (the security information is case sensitive). If you have forgotten your security information, you can have the hint emailed to you (see section 33.2.2, page 114). If you attempt the retrieval three times without success, your password will need to be reset by a PSC who can maintain your details. If a PSC cannot maintain your details, you should contact your sponsor, if you have one, or the service desk.

Issue and description	Action
Password issues	
Password forgotten You cannot remember your password.	You should inform a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor, if you have one, or the service desk. They will be able to reset your password. You will receive a new email with a unique URL to retrieve your new password. If you have also forgotten your security information that is required for the retrieval you will have to have this reset as well.
Incorrect password entered You have entered an incorrect password. The web channel returned an error.	You must enter your password again. Check you are using the correct case (the field is case sensitive).
Incorrect password entered repeatedly You have entered the wrong password consecutively and you are automatically suspended for ASM.	If you know your password, you should contact a PSC who can maintain your details. If a PSC cannot maintain your details, contact your sponsor (if you have one) or the service desk to get reinstated. If you have forgotten your password, they will have to reinstate you and reset your password. If you have also forgotten your security information they will have to reset your security information and hint reset.
Password has been compromised You know or think that someone else knows your password.	You must contact the service desk or your sponsor, if you have one, immediately. Your password should be reset.

35 ASM statuses

If you have been set up for ASM security, you will have an ASM security status. To use your contact ID and password, you will need to have an ASM status of “Active”. There are other possible statuses that you could have. The following table details the possible statuses that you may have for ASM security, and what it means if you have that status.

Status	What it means
Not set	You have not been set up to have ASM details for accessing BACS payment services.
Active	You can use your contact ID and password for everything you have been set up to do that can be accessed with ASM.
ASM pending	You have not yet retrieved your contact ID and password. For details of how to retrieve your contact ID and password see section 33.2.2, page 114.
Suspended	You cannot log on or perform any action using your contact ID and password. The status of “Suspended” may have been automatically generated by the BACS payment services system following an incident, or may have been set by your sponsor (if you have one) or a PSC who can amend your details, through the process of suspending a contact. If you also have a smartcard, providing your PKI status is “active”, you can continue to carry out everything you have been set up to do using your smartcard. If you only have ASM security, or if your PKI status is also “Suspended”, you will no longer receive any notification emails.
Suspended - Pending	As for “Suspended”, you cannot log on or perform any action using your contact ID and password. You were in a state of “ASM pending” before you were suspended, and, if you are reinstated, your status will revert to “ASM Pending”. If you also have PKI credentials, providing your PKI status is “Active”, you can continue to carry out everything you have been set up to do using your smartcard. If you only have ASM security, or if your PKI status is also “Suspended”, you will no longer receive any notification emails.

Part XII

Your details

36 Changing your details

36.1 Overview

As a contact, certain information is registered on the payment services web channel about you. This information is used in relation to your use of the payment services and includes contact information, privileges, and security information.

You can view some of this information, and change some of it. The following sections detail the information that is held about you, what that information is used for and how you can change some of that information.

36.2 How to change your details

The following procedure details how to change your contact details and your security information and hint (if you have ASM security).

To view and amend your details

You must have logged in to the web channel (with PKI or ASM) and you can view the menu.

1 Click *My details* in the left hand menu. *My details* screen loads.

The *My details* screen loads showing *Contact details* and *Privileges*.

The *Contact details* block contains, amongst other things, the following information:

- Title, first name and surname
- Security method, PKI status and ASM status
- Type
- Email address
- Office telephone number and additional information
- Out of office telephone number
- Mobile telephone number and additional information
- Fax number
- If you have ASM, there will also be a *change password* button.

The *Privileges* block(s) show the privilege groups you have been allocated.

Having viewed the information, if you wish to exit this screen, click the *cancel* button. You will be asked if you want to abandon this activity. Click *yes* to exit the contact details section.

To change any of this information go to step 2.

2 Make the required changes

To change you contact information (email address, telephone number etc):

- Highlight the information in the field you want to change
- Type the new contact information in the field
- Make further alterations (see below) or go to step 3.

To view and amend your details (continued)

To change your password (applicable to contacts with ASM):

- Click the *change password* button
- The *Change password* screen loads
- Enter your current password
- Enter what you would like as your new password in the two separate fields. For more information on the required format for your password see sec 33.5.2, pg 122
- Click *OK*
- *My details* screen reloads and your password has been changed
- Make further alterations (see below) or go to step 3.

3 Confirm your changes

Once you have made your changes, click *submit*. Go to step 4.

If you do not want to make any changes, or you want to lose the changes you have made, or all you have changed is your password (which took immediate effect), click *cancel*. You will then be asked if you wish to abandon the activity.

4 A summary screen loads. Check the details and, if correct, click *confirm*

A summary screen loads displaying the details that will be applied. If these are correct, click *confirm*. Go to step 5.

If they are not correct, or you wish to make further changes, click *back* to return to the *My details* screen and go back to step 2.

5 *Confirmation* screen loads. Authenticate yourself to make the changes.

In order to action the changes, you must authenticate yourself using the same security method you used to log on to the web channel.

If you logged on using your smartcard you must sign the text, that details the changes you are making, using your signing software.

If you logged on using your contact ID and password, enter your password and click *submit*. *Note:* if you changed your password during this procedure you must use your new password.

6 *Success* screen loads.

If the changes were made successfully, the *Success* screen loads.

Glossary

BACS

account limit	The maximum value that can be paid from (credits) or collected into (debits) an individual account or group of accounts during a period set by your sponsor without creating an overlimit referral. The account limit is set by your sponsor.
account section	The payment instructions in a payment file that have the same originating account details and are to be processed on the same processing date. A payment file can contain one or many account sections.
ADDACS (Automated Direct Debit Amendment and Cancellation Service)	The service allowing banks/building societies to advise Direct Debit originators of any amendments to or cancellations of Direct Debit Instructions.
additional contact	A type of contact able to act for a service user on BACSTEL-IP. Additional contacts cannot be given any privileges to maintain their service user or other contacts.
adjustment item	A payment instruction that the BACS service generates to ensure that account sections balance after a payment instruction(s) is rejected. The adjustment item uses the main account details for the originating and destination sorting code and account number.
allowed transaction	The name given to a transaction code that a service user is allowed to use in payment instructions they originate from a specific nominated account.
alternative security method (ASM)	An access method using a contact ID and password to provide secure access to the BACS payment services website. (To do certain things on the website, you need to use public key infrastructure, PKI, security.)
ARUCS (automated return of unapplied credits service)	The service allowing banks/building societies to return to the originator any credit payment instructions they could not apply. The credit is returned to the originator's account. Details of the credit, including the reason it has been returned, are included in an ARUCS report made available to the originator.
ARUDD (automated return of unpaid Direct Debits)	The service allowing banks/building societies to return to the originator any Direct Debit payment instructions they could not apply. The debit is returned to the originator's account. Details of the debit, including the reason it has been returned, are included in an ARUDD report made available to the originator.
AUDDIS (Automated Direct Debit Instruction Service)	The service enabling Direct Debit Instructions (DDIs) to be transferred electronically from originators to the paying banks and building societies via the BACS service.
AWACS (advice of wrong account for automated credits service)	A group of messaging services to inform originators quoting incorrect destination account details in their payments of the correct account details to use in the future.
BACS Approved Software Service for BACSTEL-IP	An approval service to make sure that all software used with BACSTEL-IP meets set requirements. You can only use software to access BACSTEL-IP that is approved under this service.
payment services	A secure website used by service users to get their reports, view their submission information and manage their contacts.

Bacstel-IP	A service providing a secure access for the Bacs service. It uses internet technologies and PKI security. You access Bacstel-IP either using payment services or Bacs approved software for Bacstel-IP.
Bacstel-IP software	In this guide, Bacstel-IP software refers to software that has been approved under the Bacs Approved Software Service for Bacstel-IP.
bureau	A bureau submits payment files to the Bacs service for other service users. Bureaux that submit for third parties must be certified as a Bacs Approved Bureau. A bureau is a type of direct submitter.
certificate authority	A trusted authority responsible for assigning digital certificates as part of PKI (public key infrastructure) security.
contact	A person that can act for a service user. There are two types of contacts: primary security contacts (PSCs) and additional contacts.
contact ID	This is used to identify a contact when they are logging on with the alternative security method (ASM).
contra	A type of payment instruction used to balance credit and debit payment instructions in an account section.
day section	The payment instructions in a payment file that are to be processed on the same day. A day section may contain one or more account sections.
destination account	The account to which a payment instruction is direct.
digital certificate	Assigned by a trusted certificate authority, a digital certificate is the form in which PKI credentials are issued. In Bacstel-IP terms, certificates are normally held on a smartcard, but can also be held on an HSM (hardware security module).
digitally sign	You digitally sign information using a smartcard or an HSM. This produces a digital signature that is attached to the file or message before it is sent. This digital signature allows the receiver to identify the sender and tell if the contents of the file or message have been altered after it was signed.
Direct Debit Instruction (DDI)	Sent by the originator to the payer's bank/building society as the authority to pay Direct Debits from the payer's account. These are set up electronically via the Bacs service if the originator uses Auddis.
direct submitter	A service user that sends payment information directly to the Bacs service. A direct submitter (that is not a bureau) also originates payment information.
electronic funds transfer (EFT)	The service that allows the movement of money from one account to another electronically.
hardware security module (HSM)	A piece of hardware installed into your computer systems that holds PKI credentials. HSMs allow you to automate the submission and report collection process.
indirect submitter	A service user that can originate payment information, but does not send it to Bacs itself. It uses a bureau to send the payment information.
input report	A report that the Bacs service produces following the processing of payment information for a particular service user for a particular day. Any payments that have been amended, rejected or returned are highlighted on the report. Using Bacstel-IP, you can access input reports within 4 hours of processing.

item limit	The maximum value an individual payment instruction can have without the payment being highlighted on the user's input report. Item limits are set by the sponsor for credit items and debit items.
modulus check	A process to check if a particular account number could exist at a given sorting code. BACSTEL-IP software modulus checks payment information before it sends it for processing.
organisation	Used in BACSTEL-IP to link associated service users.
originator	A service user that originates payment instructions. The payment instructions are originated from bank/building society accounts held by the originator.
payment file	A set of payment instructions that are submitted to the BACS service for processing. A payment file is sent as part of a submission. You can optionally digitally sign payment files.
payment instruction	A data record that effects the movement of money from one account to another or that lodges a Direct Debit Instruction at a destination bank/building society account.
primary security contact (PSC)	A type of contact linked to a service user. Direct submitters must have at least two PSCs; indirect submitters do not have to have any PSCs. A PSC can be given a wider range of privileges than an additional contact, including the privilege to be able to add and maintain additional contacts.
processing day	Any calendar day except Saturdays, Sundays and English bank/public holidays.
public key infrastructure (PKI)	A system to verify the validity of parties involved in electronic communications and to secure electronic data transmissions. PKI uses two "keys": a public and a private key. A message encrypted with a private key can only be decrypted with the associated public key (and vice versa).
public key infrastructure (PKI) credentials	The collective term for the public and private keys issued to an individual in the form of a digital certificate. PKI credentials are used for authentication and encryption. They are issued by a trusted certificate authority.
service qualification plan	The testing programme linked to a service user's BACSTEL-IP software.
service user	A company, group of companies, charity etc that is sponsored to use the BACS service.
service user number	A number allocated to a service user to uniquely identify it. A service user number is six numerals (or for a bureau, a B followed by five numerals).
smartcard	A card with an embedded microchip that is used to store a contact's PKI credentials. The smartcard is used to authenticate the holder and digitally sign data.
software supplier	In this guide, software supplier refers to the provider of your BACSTEL-IP software.
sponsor	The bank or building society that has authorised your service user to use the BACS service.
submission	A payment file or files transmitted to the BACS service for processing. All submissions sent to BACSTEL-IP must be digitally signed using PKI credentials.
XML (extensible markup language)	A computer language allowing data to be associated with instructions for processing the data. Reports on BACSTEL-IP can be accessed in XML format. This allows you to upload the reports into other applications.